Wyzwania systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu

pod redakcją naukową
Pawła Gołębiewskiego
Pawła Sitka

WYDAWNICTWO
AEH

Wyzwania systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Wyzwania systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu

pod redakcją naukową
Pawła Gołębiewskiego
Pawła Sitka

WYDAWNICTWO
AEH

Warszawa 2021

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Akademia Ekonomiczno-Humanistyczna w Warszawie

Recenzenci
prof. dr hab. Mirosław Karpiuk
dr hab. Jarosław Kostrubiec, prof. UMCS

Copyright © 2021 by Akademia Ekonomiczno-Humanistyczna w Warszawie

Redaktor prowadzący
Wojciech Żyłko

Redakcja i korekta
Studio F

Projekt okładki
Studio F

Skład i łamanie
Studio F

ISBN 978-83-66552-42-5

Wydawnictwo
Akademii Ekonomiczno-Humanistycznej
ul. Okopowa 59
01-043 Warszawa

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Poszczególne rozdziały opracowali i napisali:

Paweł Sitek: rozdział 1 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Izabela Juhnke: rozdział 2 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Justyna Gryniuk: rozdział 3 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Adam Krupa: rozdział 4 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Mateusz Ficygowski: rozdział 5 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Witold Wyporek: rozdział 6 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Adam Życzkowski: rozdział 7 (Wyższa Szkoła Gospodarki Euroregionalnej w Józefowie)

Tomasz Talar: rozdział 8 (Wyższa Szkoła Gospodarki Euroregionalnej w Józefowie)

Radosław Sałatka: rozdział 9 (Wyższa Szkoła Gospodarki Euroregionalnej w Józefowie)

Anna Samrau: rozdział 10 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Katarzyna Chudzik: rozdział 11 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Paweł Piotrowski: rozdział 12 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Paweł Gołębiewski: rozdział 13 (Akademia Ekonomiczno-Humanistyczna w Warszawie, Instytut Nauk Prawnych)

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

SPIS TREŚCI

Wykaz skrótów 11
Przedmowa 15

ROZDZIAŁ 1. STABILNOŚĆ FINANSOWA PAŃSTWA A SYSTEM AML
(*Paweł Sitek*) 19

1.1. Uwagi wprowadzające 19
1.2. Stabilność finansowa państwa 22
1.3. Działania NBP na rzecz stabilności krajowego systemu finansowego 27
1.4. Wpływ i znaczenie systemu AML na stabilność finansową państwa 29
1.5. Podsumowanie 37

ROZDZIAŁ 2. MLRO – *MONEY LAUNDERING REPORTING OFFICER* – OSOBISTA ODPOWIEDZIALNOŚĆ CZŁONKÓW ZARZĄDU WEDŁUG USTAWY AML/CFT
(*Izabela Juhnke*) 41

2.1. Uwagi wprowadzające 41
2.2. Powołanie AMLO, MLRO 42
2.3. Obowiązki AMLO, MLRO 47
2.4. Odpowiedzialność AMLO, MLRO 51
2.5. Podsumowanie 60

ROZDZIAŁ 3. PROBLEMATYKA IDENTYFIKACJI BENEFICJENTA RZECZYWISTEGO
(*Justyna Gryniuk*) 61

3.1. Uwagi wprowadzające 61
3.2. Kto jest uznawany za beneficjenta rzeczywistego? 62
3.3. Środki bezpieczeństwa finansowego 64
3.4. Identyfikacja beneficjenta rzeczywistego 65

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

3.5. Osoby zajmujące eksponowane stanowiska polityczne 67
3.6. Centralny rejestr beneficjentów rzeczywistych 70
3.7. Wymóg niekaralności beneficjenta rzeczywistego 74
3.8. Podsumowanie 76

ROZDZIAŁ 4. ANALIZA RYZYKA – PROBLEMATYKA OUTSOURCINGU PROCESÓW ZWIĄZANYCH Z AML/CFT
(*Adam Krupa*) 79

4.1. Uwagi wprowadzające 79
4.2. Charakter prawny umowy dotyczącej outsourcingu 81
4.3. Ramy prawne outsourcingu w systemie bezpieczeństwa finansowego 82
4.4. Outsourcing procesów związanych z bezpieczeństwem finansowym w wybranych instytucjach obowiązanych 85
4.5. Podsumowanie 93

ROZDZIAŁ 5. SHELL COMPANIES, OBOWIĄZKI INSTYTUCJI OBOWIĄZANYCH
(*Mateusz Ficygowski*) 97

5.1. Uwagi wstępne 97
5.2. Shell Companies 98
5.3. Instytucje obowiązane 101
5.4. Środki bezpieczeństwa finansowego 106
5.5. Transakcje podejrzane 111
5.6. Podsumowanie 114

ROZDZIAŁ 6. FINTECH, GLOBALIZACJA USŁUG A KRAJOWE REGULACJE
(*Witold Wyporek*) 117

6.1. Uwagi wprowadzające 117
6.2. Nadzór i kontrola sektora FinTech 120
6.3. Ryzyko usług sektora FinTech a przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu. *Anti-Money Laundering/Combating the Financing of Terrorism* (AML/CFT) 124
6.4. Globalne zagrożenia i wyzwania regulacji w obszarze sektora FinTech i funkcjonowania obowiązanych instytucji finansowych 134
6.5. Podsumowanie 140

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ROZDZIAŁ 7. ROZWÓJ ZAUTOMATYZOWANYCH TECHNOLOGII WSPIERAJĄCYCH AML I CFT
(*Adam Życzkowski*) 143

7.1. Uwagi wprowadzające 143
7.2. Zmiany prawne na poziomie europejskim i krajowym 145
7.3. Główne trendy w innowacjach cyfrowych 147
7.4. Strategiczne cele finansów cyfrowych na podstawie propozycji KE 149
7.5. Priorytety i powiązane działania, aby umożliwić konsumentom i przedsiębiorstwom czerpanie korzyści z technologii cyfrowych finansów 151
7.6. Rozwój zautomatyzowanych technologii wspierających AML i CFT 153
7.7. Wyzwania związane z cyfryzacją i ochroną danych osobowych 157
7.8. Zautomatyzowane funkcjonalności w zakresie AML 158
7.9. AI via AML 159
7.10. Podsumowanie 160

ROZDZIAŁ 8. PROCEDURA AML W BIURACH RACHUNKOWYCH – WYBRANE ASPEKTY
(*Tomasz Talar*) 163

8.1. Uwagi wprowadzające 163
8.2. Biura rachunkowe jako instytucja obowiązana 164
8.3. Ogólna ocena ryzyka w biurze rachunkowym 167
8.4. Rozpoznawanie ryzyka prania pieniędzy oraz finansowania terroryzmu w biurach rachunkowych 171
8.5. Środki bezpieczeństwa finansowego w biurze rachunkowym 173
8.6. Wewnętrzna procedura biura rachunkowego w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu 179
8.7. Informacje o transakcjach ponadprogowych w biurze rachunkowym 180
8.8. Podsumowanie 182

ROZDZIAŁ 9. OBOWIĄZKI KONTROLNE STAROSTY WOBEC FUNDACJI I STOWARZYSZEŃ W ZWIĄZKU Z USTAWĄ O PRZECIWDZIAŁANIU PRANIU PIENIĘDZY ORAZ FINANSOWANIU TERRORYZMU
(*Radosław Sałata*) 185

9.1. Uwagi wprowadzające 185
9.2. Ustawowy obowiązek kontroli stowarzyszeń i fundacji przez starostę 186
9.3. Wewnętrzne procedury AML w starostwie powiatowym 193
9.4. Podsumowanie 197

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ROZDZIAŁ 10. NARZĘDZIA ORGANÓW PAŃSTWOWYCH I PODATKOWYCH W WALCE Z PRANIEM PIENIĘDZY (*Anna Samrau*) 201

10.1. Uwagi wprowadzające 201
10.2. Organy instytucjonalne zajmujące się przeciwdziałaniem praniu brudnych pieniędzy 203
10.2.1. Generalny Inspektor Informacji Finansowej 205
10.2.2. Jednostki współpracujące (organy podatkowe i celne) 209
10.2.3. Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu 211
10.3. Organy podatkowe w walce z przestępczością prania pieniędzy 213
10.3.1. Krajowa Administracja Skarbowa 214
10.3.2. Czynności operacyjno-rozpoznawcze organów Krajowej Administracji Skarbowej 216
10.4. Blokada rachunku bankowego podmiotu kwalifikowanego 217
10.5. Jednolity plik kontrolny 218
10.6. Mechanizm podzielnej płatności 219
10.7. Podsumowanie 220

ROZDZIAŁ 11. WSTRZYMANIE TRANSAKCJI I BLOKADA RACHUNKU JAKO NARZĘDZIA WALKI Z ML/FT (*Katarzyna Chudzik*) 223

11.1. Uwagi wprowadzające 223
11.2. Wstrzymanie transakcji i blokada rachunku w Ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu 225
11.3. Wstrzymanie transakcji i blokada rachunku w prawie bankowym 229
11.4. Wykorzystanie przez państwo blokady rachunku i wstrzymania transakcji 233
11.5. Podsumowanie 237

ROZDZIAŁ 12. PROBLEMATYKA EGZEKUCJI KAR ADMINISTRACYJNYCH NAKŁADANYCH NA PODSTAWIE USTAWY AML/CFT (*Paweł Piotrowski*) 239

12.1. Uwagi wprowadzające 239
12.2. Kary administracyjne 240
12.3. Katalog kar administracyjnych 243
12.4. Rodzaj kary 247
12.5. Czynniki mające wpływ na wysokość kary 248
12.6. Egzekucja i ich rodzaje 249
12.7. Po co jest egzekucja i kto może prowadzić postępowanie 251
12.8. Podsumowanie 255

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ROZDZIAŁ 13. ODPOWIEDZIALNOŚĆ KARNA OSÓB DZIAŁAJĄCYCH W IMIENIU LUB NA RZECZ INSTYTUCJI OBOWIĄZANEJ
(*Paweł Gołębiewski*) 257

13.1. Uwagi wprowadzające 257
13.2. Międzynarodowe działania na rzecz AML/CFT 259
13.3. Karne regulacje za delikty w ustawie AML/CFT 264
13.4. Skazanie na podstawie ustawy AML/CFT a piastowanie funkcji lub stanowiska w podmiotach gospodarczych 272
13.5. Działania kontrolne Generalnego Inspektora 282
13.6. Podsumowanie 284

Literatura 175

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Wykaz skrótów

(AIS) – dostęp do informacji o rachunku

(PIS) – inicjowanie płatności

5G – technologia uznawana za najnowszą, piątą generację sieci komórkowej

ABW – Agencja Bezpieczeństwa Wewnętrznego

AI – sztuczna inteligencja (ang. *artificial intelligence*, niem. *künstliche intelligenz*)

AML – przeciwdziałanie praniu pieniędzy (*anti-money laundering*)

AML/CTF – przeciwdziałanie praniu pieniędzy i przeciwdziałanie finansowaniu terroryzmu.

AMLCO – Approved AML Compliance Officer

AMLO/AMCLO – *Anti Money Laudering Officer/Anti Money Laudering Compliance Officer*, czyli oficer ds. zgodności z ustawą o przeciwdziałaniu praniu pieniędzy.

art. – artykuł

B2B – wymiana handlowa pomiędzy przedsiębiorcami (*Business-to-business*)

B2C – wymiana handlowa pomiędzy przedsiębiorcą a konsumentem (*Business-to--consumer*)

BigTech – zbiorcze określenie na dominujących amerykańskich gigantów z branży IT

BigTech – część sektora FinTech obejmująca funkcjonowanie gigantów branży innowacyjności technologicznych i technologii finansowych

BIP – Biuletyn Informacji Publicznej

BLIK – system płatności mobilnych

BSBC – Bazylejski Komitet ds. Nadzoru Bankowego (Basel Committee on Banking Supervision)

CBA – Centralne Biuro Antykorupcyjne

CRBR – Centralny Rejestr Beneficjentów

D.U. – Dziennik Urzędowy Rzeczypospolitej Polskiej

DLT Blockchain – kryptograficzna baza danych rozproszonego rejestru

DMLO – *Deputy Money Laundering Officer*, czyli zastępca AMLO

DORA – Digital Operational Resilience Act

Dz.U. – dziennik Ustaw

EBA – Europejski Urząd Nadzoru Bankowego

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

EIOPA – Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych

ESMA – Europejski Urząd Nadzoru Giełd i Papierów Wartościowych

EUNB – Europejski Urząd Nadzoru Bankowego

EUR – waluta euro

FATF – Międzynarodowa organizacja rządowa ds. przeciwdziałania praniu pieniędzy (Financial Action Task Force)

FinTech – Technologie Finansowe (*financial technology*).

FinTech Startup – nowopowstała firma wykorzystująca technologie finansowe

FIU – jednostki analityki finansowej (Financial Intelligence Unit)

FT – finansowanie terroryzmu (*terrorism financing*)

GIIF – Generalny Inspektor Informacji Finansowej

HCE – pozwala na szybkie, zbliżeniowe płatności telefonem na podobnej zasadzie jak w przypadku karty płatniczej (*Host Card Emulation*)

iAML – system analityczno-raportującywspierający przeciwdziałanie praniu pieniędzy

ICT – technologie informacyjno-komunikacyjne

IoT – internet rzeczy, internet przedmiotów (ang. internet of things, IoT)

IoT – *Internet of Things* lub *Intelligence of Things*

IT – dyscyplina informatyczna i branża na rynku pracy zajmująca się stosowaniem technologii obliczeniowych

IVDAML – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE

k.k. – Kodeks Karny

k.p. – Kodeks Pracy

k.s.h. – Kodeks spółek handlowych

KAS – Krajowa Administracja Skarbowa

KBF – Komitet Bezpieczeństwa Finansowego

KE – Komisja Europejska

KNF – Komisja Nadzoru Finansowego

Kpc – Kodeks postępowania cywilnego

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Ksh – Kodeks spółek handlowych

KYC – zbiór informacji o kliencie, który pozwala ustalić wiarygodność klienta i jego profil transakcyjny

KYC – poznaj swojego klienta, procedura starannej identyfikacji klienta (*know your customer*)

MF – Minister Finansów

ML – pranie pieniędzy (*money laundering*)

ML/FT – pranie pieniędzy i finansowanie terroryzmu

MLRO – czyli oficer raportowania transakcji (*Money Laundering Reporting Officer*)

moBILET – platforma płatności mobilnych

mPay – uniwersalny system płatności mobilnych

N26 – bank, który działa wyłącznie online

NBP – Narodowy Bank Polski

NIK – Najwyższa Izba Kontroli

OC – czyli oficer ds. zgodności (*Compliance Officer*)

ONZ – Organizacja Narodów Zjednoczonych

Organizacja non-profit – pozarządowa organizacja, której celem nie jest osiągnięcie zysku, a jej dochody są przeznaczane na finansowanie działalności

P2P – Peer to Peer, połączenie internetowe pomiędzy klientami bezpośrednie, bez potrzeby korzystania z serwera głównego

PEP – osoby zajmujące eksponowane stanowiska polityczne

poz. – pozycja

RegTech – Technologia Regulacyjna dla sektora finansowego wykorzystująca nowoczesne technologie do lepszego adoptowania funkcjonowania podmiotów obrotu gospodarczego w zakresie wymogów ustawodawczych

Revolut – aplikacja do płatności wielowalutowych

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

SAS – *single attached stations*

SG – Służba Graniczna

SkyCash – platforma płatności mobilnych umożliwiająca zakup m.in. biletów kolejowych i komunikacji miejskiej

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

soft law – prawo miękkie

SSL – protokół sieciowy używany do bezpiecznych połączeń internetowych

SupTech – branża funkcjonująca w FinTech zajmująca się gromadzeniem, analizą i przetwarzaniem danych na potrzeby sektora FinTech i wymogów ustawodawczych

Twisto – usługa, która łączy w sobie zalety karty kredytowej, kredytu odnawialnego oraz oferty ratalnej

u.p.b. – Ustawa Prawo Bankowe

u.p.p.p.f.t. – Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

UE – Unia Europejska

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

PRZEDMOWA

Współpraca opierająca się na zrozumieniu wspólnych celów w wielu obszarach działalności człowieka daje korzystniejsze efekty niż ustanowiony system kar, które grożą danemu podmiotowi w przypadku naruszenia określonych obowiązków lub zaniechania kooperacji, którą z należytą starannością winien wykonywać. Zrozumienie problematyki, a co z tym powinno się wiązać właściwy system wartościowania wspólnych dóbr, umiejętność współpracy, efektywne współdziałanie, są kluczem do sukcesu na wielu polach.

Pranie pieniędzy, które można odmieniać przez wiele przypadków, w rzeczywistości brzmi obco dla osoby, której wydaje się, że nie jest w stanie swoim działaniem przeciwdziałać temu zjawisku. Czasami w wątpliwość podaje się jego istotę lub negatywne działanie. To pierwszy element, który może powodować zaniedbanie nałożonych ustawowo obowiązków. Drugi, to ignorowanie problematyki. Wszak najczęściej może wydawać się, iż fakt, że ktoś, kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, przekazuje lub wywozi za granicę, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, tak naprawdę nie wpływa na codzienne życie czy stabilność całego systemu finansowego.

Odmiennie może być kojarzone zjawisko finansowania terroryzmu określone w art. 165a k.k. W tym przypadku, mimo iż skala negatywnego działania nie jest odbiorcy do końca znana, brzmi na tyle groźnie, iż każdy będzie miał wzmożoną czujność w tym obszarze.

Słownik języka polskiego jako system określa:

- układ elementów mający określoną strukturę i stanowiący logicznie uporządkowaną całość,
- zespół wielu urządzeń, dróg, przewodów itp., funkcjonujących jako całość,
- narządy lub inne części żywego organizmu pełniące razem określoną funkcję,
- uporządkowany zbiór twierdzeń, poglądów, tworzących jakąś teorię,
- określony sposób wykonywania jakiejś czynności lub zasady organizacji czegoś,
- zespół skał powstałych w ciągu jednego okresu geologicznego,

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- *log.* całościowy i uporządkowany zespół zdań połączonych ze sobą stosunkami logicznego wynikania[1].

W każdej z definicji wyrazu kładzie się nacisk na współdziałanie, uporządkowanie. Podobnie należy postrzegać system przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Jego kształt wyznaczają przede wszystkim przepisy prawne, zarówno krajowe, jak i Unii Europejskiej. Podstawowym aktem prawnym w tym obszarze jest ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723 ze zm.). Wskazuje ona organy i podmioty funkcjonujące w ramach tego systemu oraz określa ich obowiązki i uprawnienia.

Centralnym elementem polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu jest Generalny Inspektor Informacji Finansowej, usytuowany w Ministerstwie Finansów.

Instytucje obowiązane to w dużym uproszczeniu podmioty szeroko rozumianego sektora finansowego, jak również wykonujące określone w ustawie czynności związane z obrotem pieniężnym czy też usługami w tym zakresie. Ich zadanie w omawianym systemie to rozpoznawanie i ocena ryzyka prania pieniędzy oraz finansowania terroryzmu związanego ze stosunkami gospodarczymi zawieranymi z klientami lub z transakcjami okazjonalnymi realizowanymi przez nich. Ponadto podmioty te na bazie tego ryzyka i jego oceny stosują środki bezpieczeństwa finansowego, których zadaniem jest przede wszystkim uzyskanie informacji na temat ich klientów oraz celu, dla którego korzystają oni z usług i produktów oferowanych przez instytucje obowiązane. Instytucje te są zobowiązane do zawiadamiania Generalnego Inspektora o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, jak również o przypadkach powzięcia uzasadnionego podejrzenia, że określona transakcja lub wartości majątkowe mogą mieć związek z wymienionymi czynami zabronionymi.

Ostatnim elementem systemu są jednostki współpracujące, które również są zobowiązane do współpracy z GIIF i powiadamiania go o podejrzeniu popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu. Dodatkowo jednostki te dla realizacji celów ustawowych mogą uzyskiwać informacje gromadzone przez Generalnego Inspektora. Wszystkie wymienione elementy muszą ze sobą współgrać dla stabilności systemu.

Przestępstwa prania pieniędzy lub finansowania terroryzmu mają najczęściej wymiar międzynarodowy, co oznacza, iż tworzony w Polsce system oraz jego stabilność ma wpływ i istotne znaczenie dla innych krajów i ich systemów.

Z tego też powodu zostały stworzone instytucje międzyrządowe, mające na celu wypracowywanie i określanie standardów istotnych dla przeciwdziałania praniu

[1] https://sjp.pwn.pl/ (data dostępu: 26.9.2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

pieniędzy oraz finansowaniu terroryzmu, w szczególności Financial Action Task Force (Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy), która opracowała poruszane w książce rekomendacje. Dokument ten tworzy pełny i spójny zespół środków, który powinien zostać implementowany przez poszczególne kraje w celu zwalczania prania pieniędzy, finansowania terroryzmu, a także finansowania proliferacji broni masowego rażenia. Również zostały stworzone instytucje kontrolne, jak choćby Moneyval, jako Komitet Ekspertów ds. Oceny Środków Przeciwdziałania Praniu Pieniędzy i Finansowania Terroryzmu, który jest organem monitorującym Rady Europy i w drodze ewaluacji weryfikuje, czy jego państwa członkowskie posiadają efektywne systemy przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu, zgodne z odpowiednimi standardami.

Podkreślić należy, iż współdziałanie wszystkich ogniw systemu na podstawie jasnych i czytelnych zasad jest kluczem do jego stabilności, jednak pojawiają się wątpliwości i pytania co do funkcjonowania systemu oraz nałożonych na jego członków obowiązków, które są poruszane w niniejszej pracy. Wskazać należy, iż autorzy książki w swoich pracach prowadzą rozważania, które opierają nie tylko na wiedzy teoretycznej, ale również na praktycznych aspektach związanych z funkcjonowaniem jako część systemu – w instytucjach obowiązanych, czy też jednostkach współpracujących. Poruszane przez nich kwestie związane są niejednokrotnie z nowymi pojawiającymi się elementami systemu, które wynikają z nowelizacji aktów prawnych, ale również przemian w gospodarce związanej na przykład z rozwojem fintechu i ryzyka, jakie mogą się pojawić. Stawiane w książce tezy wychodzą naprzeciw oczekiwaniom biznesu, który z uwagi na możliwe delikty, poprzez procedury zgodnościowe, a także tworzenie stanowisk *Compliance Officer,* stara się dbać o wdrażanie niezbędnych zasad i ich bieżącego przestrzegania. Być może jednak, należałoby przychylić się do rozważań nad znaczeniem technologii, która również może przysłużyć się skutecznym procedurom. Poruszane w pracy rozważania autorów w zakresie sztucznej inteligencji i zastosowania algorytmów uczenia się do oceny i analizy ryzyka również mogą świadczyć o kolejnym przełomie w budowaniu stabilności systemu.

Praca stara się odpowiadać nie tylko na zasady już ustanowione. Refleksje zawarte w kolejnych rozdziałach książki nawiązują do istotnych pytań w zakresie zasadnych do przeprowadzenia zmian w prawie, jak i zmian organizacyjnych w instytucjach obowiązanych, podnoszących poziom spójności systemu oraz jego kluczowych narzędzi, których zrozumienie przez współdziałanie zmniejszy podatność naszego systemu finansowego na wykorzystanie go do przestępczych celów.

Paweł Gołębiewski

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Paweł Sitek
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 1.

STABILNOŚĆ FINANSOWA PAŃSTWA A SYSTEM AML

1.1. UWAGI WPROWADZAJĄCE

Wybór problemu badań do tego rozdziału wprost wynika z ogólnej koncepcji niniejszej monografii. Współczesne wyzwania w zakresie stabilności systemu przeciwdziałania praniu pieniędzy i zwalczaniu terroryzmu (AML/CFT) wynikają i bezpośrednio wpływają na potrzebę zapewniania i podnoszenia bezpieczeństwa państwa, w szczególności jego stabilności finansowej. Jednocześnie geneza niniejszej monografii wynika z faktu, że polski ustawodawca uchwalając ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu dokonał implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającej rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającej dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz. Urz. UE L 141 z 5 czerwca 2015 r., s. 73, Dz. Urz. UE L 156 z 19 czerwca 2018 r., s. 43 oraz Dz. Urz. UE L 334 z 27 grudnia 2019 r., s. 155).

Celem niniejszego rozdziału jest podjęcie próby ustalenia współczesnych komponentów pojęcia stabilności finansowej i wielopłaszczyznowości jego rozumienia oraz wskazanie na możliwe źródła jego ujęcia, a przez to również przybliżenie zmiany układu sieci stabilności finansowej w architekturze finansowej UE przez zmianę akcentu normatywnego w poszczególnych elementach tej sieci. Jednocześnie przeanalizowanie roli przepisów dotyczących przeciwdziałaniu

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

praniu pieniędzy i zwalczania terroryzmu w związku z koniecznością zapewnienia stabilności finansowej państwa[1].

Podstawową tezą niniejszego rozdziału jest twierdzenie, że stabilność finansowej jest wieloelementowym i wielopłaszczyznowym oraz wielofunkcyjnym pojęciem, odnoszonym na szczeblu UE i krajowym zarówno do rynku jako całości, instytucji finansowych, jak i państwa. W rozdziale został omówiony i przeanalizowany pogląd o możliwości urzeczywistnienia stabilności finansowej jako wypadkowej wyważenia, pogodzenia i urzeczywistniania interesów prawnych wszystkich uczestników rynku finansowego (w tym również organów reprezentujących państwo), a wpisuje się również w pojęciowe poszukiwania w ramach podejmowanej w dyskursie teorii prawa rynku finansowego UE.

Można przyjąć, że stabilność finansowa państwa to obraz złożony z odpowiednio rozumianej stabilności finansowej rynku finansowego oraz odpowiednio rozumianej stabilności bezpieczeństwa wymaganych od państwa. Rynek finansowy nie jest realizowany w ramach bezwzględnie rozumianej zasady wolności gospodarczej. Przeciwnie, jest tak newralgiczny, iż instytucje państwa (organy państwa) występują w roli podmiotów kreujących określone procesy, regulujące i kontrolujące te procesy oraz udzielające zezwoleń na prowadzenie działalności na rynkach finansowych.

Należy zgodzić się z poglądem, że istnienie stabilnego, efektywnego systemu finansowego uwarunkowane jest wieloma czynnikami, uzależnionymi (stanowiącymi wypadkową) od aktywności państwa[2]. Państwa, w którym kolejno są zagwarantowane poszczególne poziomy bezpieczeństwa: (ze względu na dziedzinę) ekologiczne, ekonomiczne, energetyczne, informatyczne (cybernetyczne, teleinformatyczne), kulturowe, militarne, polityczne, socjalne i społeczne. Słusznie zauważa S. Szydło, że system gospodarczy obejmuje dwie sfery ludzkiej działalności: realną i finansową. Sfera realna dotyczy aspektów rzeczowych funkcjonowania podmiotów gospodarczych, a sfera finansowa tworzy ten krąg zdarzeń gospodarczych, w których następuje kreowanie pieniądza i ruch nośników jego siły nabywczej.

W naszych rozważaniach podejmiemy dalsze badania wokół rynku finansowego. A w szczególności wokół stabilnego rynku finansowego, który jest zdolny reagować na wstrząsy oraz przeciwdziałać sytuacjom nierównowagi finansowej, minimalizując ryzyko wystąpienia zakłóceń w procesie pośrednictwa finansowego.

O stabilność finansowej można mówić wówczas, gdy system finansowy wypełnia łącznie trzy swoje podstawowe funkcje, tj.:

[1] Szerzej: M. Szurek, *Pozyskiwanie śladów finansowania terroryzmu i ich przetwarzanie*, Gdańskie Wydawnictwo Oświatowe, Gdańsk 2021.

[2] S. Szydło, *Rola państwa w kształtowaniu stabilnego, efektywnego systemu finansowego*, Studia Ekonomiczne/Uniwersytet Ekonomiczny w Katowicach, Katowice 2015, nr 210, s. 231–241.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- efektywnie i sprawiedliwie alokowane są środki oszczędzających,
- właściwie szacowane i zarządzane jest ryzyko finansowe, zarówno w okresie krótkim, jak i w dłuższej perspektywie,
- szoki realne i finansowe są łagodnie absorbowane[3].

Wobec powyższego została zdefiniowana dodatkowa teza, iż zapobieganie zjawisku prania pieniędzy i finansowaniu terroryzmu jest istotnym czynnikiem wpływającym na globalne bezpieczeństwo, a w szczególności integralności systemu finansowego i zrównoważonego wzrostu.

Przedmiotowy rozdział poświęcono problematyce eliminacji zagrożenia w aspekcie podejrzenia popełnienia przestępstwa prania pieniędzy bądź finansowania terroryzmu na szczeblu krajowym i unijnym oraz realne i potencjalne zagrożenie dla stabilności finansowej.

Zjawiskiem coraz bardziej powszechnym w obecnym czasie jest wykrywalność przestępstw popełnianych nie tylko przez zwykłych obywateli, lecz także jednostki ściśle powiązane ze sferami polityki, spółek skarbu państwa. Zasadniczo przestępstwa tego rodzaju wynikają z chęci szybkiego wzbogacenia się[4]. By osiągnąć zmierzony cel jednostki uwikłane w ten proceder niejednokrotnie dopuszczają się aktów przemocy fizycznej, psychicznej, szantażu, korupcji itd. Wiadomym jest, iż wszelkie działania organizacji przestępczych, zaistniałe w celu wprowadzenia nielegalnych zysków w oficjalny obrót gospodarczy noszą miano przestępczości zorganizowanej.

Proceder prania pieniędzy stanowi poważne zagrożenie dla gospodarki i klasyfikowany jest jako przestępstwo gospodarcze. Problematyka tego zagadnienia wielokrotnie stanowiła przedmiot rozważań zarówno w ujęciu historycznym, jak i wynikających konsekwencji dla gospodarki krajowej oraz zagranicznej, o czym świadczy szeroki zakres publikacji w tym zakresie.

Z uwagi na rozmiar omawianego przestępstwa gospodarczego zarówno w ujęciu krajowym, jak i ogólnoświatowym należy wspomnieć o konsekwencjach, wynikających z jego istnienia. Należą do nich m.in.:

- zakłócenie systemu finansowego,
- zachwianie mechanizmów rynkowych,
- wzrost korupcji w państwie,
- rozwoju przestępczości zorganizowanej.

Zjawisko prania pieniędzy nie jest czynem o jednolitym charakterze, lecz składa się z wielu elementów stanowiących o złożoności tego procesu. Identyfikacja metod prania pieniędzy jest wieloraka, w oparciu o literaturę przedmiotu wyodrębnić

[3] S. Szydło, *op. cit*., s. 231–241.

[4] Szerzej: W. Kapica, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Wolters Kluwer, Warszawa 2020.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

można swoistą dwuetapowość uwzględniającą podział na pierwszy i drugi stopień tego procesu.

Pierwotny etap ma na celu utrudnić wykrycie pochodzenie określonych środków finansowych, jak również zminimalizować ślady wskazujące na jednostki bądź podmioty, od których pochodzą. W omawianym etapie zazwyczaj następuje wymiana środków finansowych na papiery wartościowe, waluty innych państw bądź transfer pieniędzy poza obszar kraju. Kolejny etap to moment, gdy zachodzi realna możliwość wskazania organom podatkowym wspomnianych środków finansowych jako pozyskane w sposób legalny oraz podlegający opodatkowaniu. Etap ten ma na celu minimalizację wszelkich śladów pochodzenia nielegalnych zysków[5].

Z uwagi na powyższe należy wspomnieć, iż w świetle ogromnej skali omawianego procederu metody przeciwdziałania muszą stanowić wiele inicjatyw międzynarodowych. System przeciwdziałania praniu pieniędzy zasadniczo oparty jest na ustawodawstwie, gdzie środki zapobiegawcze wskazują polskie regulacje prawne, regulacje Unii Europejskiej oraz regulacje o charakterze międzynarodowym. Zatem podejmowane we współpracy różnych organów działania umożliwiają ograniczenie przedmiotowego procederu. Mowa tu o działaniach banków, instytucji finansowych, służb skarbowych, działaniach międzynarodowych i krajowych służb dochodzeniowych, jak również międzynarodowych organizacji ustawodawczych. Jak już zostało wspomniane, proces prania pieniędzy ściśle związany jest z przestępczością zorganizowaną, stanowiąc finalny etap podejmowanych przez struktury przestępcze przedsięwzięć, niezależnie od wymiaru gospodarczego, kryminalnego czy narkotykowego.

1.2. STABILNOŚĆ FINANSOWA PAŃSTWA

Stabilność finansowa państwa jest pojęciem technicznym, powszechnym, zasadniczo nienormatywnym. Przyjmuje się, że stabilność finansowa odnosi się do rynku finansowego. Należy zgodzić się z profesor M. Federowicz, która zauważa, iż stabilność finansowa jest pojęciem ulegającym mocnej normatywizacji. Pojęcie stabilności finansowej występuje w rozważaniach doktrynalnych oraz w unijnym i krajowym procesie legislacji. Stąd ustalone i uznane jest rozpatrywanie stabilności finansowej rynku (finansowego) krajowego w Polsce czy UE.

Wobec tgo należy uznać, że stabilność finansowa polskiego rynku finansowego składa się z bezpieczeństwa funkcjonowania wszystkich rynków tworzących w Polsce rynek finansowy. Słusznie zauważa profesor M. Federowicz, że

[5] M.A. Kędzierski, *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce*, Adam Marszałek, Toruń 2021, s. 625 i n.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

źródło tego pojęcia wywodzi się z bankowości centralnej[6]. Bankowość centralna jako pierwsza koncentrowała się wokół stabilności cenowej i finansowej. Aktualnie termin „stabilność finansowa" jest odnoszony do nowo definiowanych obszarów i jest używany przez wielu prawodawców szczebla unijnego i krajowego. W zasadzie każdy uczestnik rynku finansowego posiada swoją cząstkę stabilności finansowej, składającą się w efekcie skali na stabilność całego systemu finansowego[7].

Z uwagi na powyższe uprawnione jest również analizowanie stabilności finansowej pod kątem państwa w rozumieniu prawa międzynarodowego. Marginalnie można zauważyć, iż wcześniej powstało pojęcie „destabilizacji finansowej państwa" i jego objawów niż zdefiniowanie stabilności finansowej państwa.

Pierwszoplanowego znaczenia stabilność finansowa nabrała dopiero w okresie ostatniego, globalnego kryzysu (2008–2014). Skala skutków kryzysu oraz odpowiednie tło polityczne w UE i na świecie spowodowała solidarną pracę nad ustaleniem przyczyn kryzysu. Następnie podjęcie działań zaradczych oraz wprowadzenie odpowiednich reform mających na celu zminimalizowanie prawdopodobieństwa wystąpienia kolejnego kryzysu, a także ograniczenie jego możliwych skutków[8].

Wstępnie można zaproponować robocze rozumienia stabilności finansowej państwa jako wypadkową wyników (poziomów bezpieczeństwa) osiąganych przez głównych uczestników poszczególnych rynków funkcjonujących w jednej przestrzeni prawodawczej np. w Polsce. Pojęcie „stabilność finansowa państwa" zmusza do postawienia pytań o potrzebę tworzenia definicji i jej treści, a przede wszystkim o potrzebę odnoszenia tego pojęcia do regulacji AML

Nurtujące jest pytanie o to, czy stabilność finansowa państwa jest celem, wartością, która ma zostać osiągnięta dzięki regulacji AML, czy AML jest wtórnym czy pierwotnym warunkiem stabilności finansowej państwa?

Stabilność finansowa dotyczy rynku jako całości. Oznacza to, że na stabilność rynku wpływ wywierają poszczególne wypadkowe stabilności pozostałych uczestników rynku finansowego kraju, Wytwarzając efekt synergii dla wspólnej stabilności finansowej państwa, rozumianej jako dobro wspólne i wspólna wartość na szeroko pojętym rynku finansowym kraju[9].

---

[6] M. Federowicz, *O normatywnym pojęciu stabilności finansowej na rynku finansowym Unii Europejskiej w nowej architekturze nadzorczej*, „Studia Europejskie" 2017, nr 4, 73–94.

[7] E. Fojcik-Mastalska, *Bank centralny. Miejsce Narodowego Banku Polskiego w sieci bezpieczeństwa finansowego* (w:) *Prawo finansowe*, red. R. Mastalski, E. Fojcik-Mastalska, Warszawa 2011, s. 455.

[8] P. Sitek, *Zintegrowany sektor bankowy Unii Europejskiej. Studium prawno-finansowe*, Vizja Press & IT, Warszawa 2015 oraz P. Sitek, *The economic security of the State and the banking union*, Lambert Academic Publishing, Saarbrücken 2015.

[9] M. Lemmonier, *Europejskie modele instrumentów finansowych*, Wolters Kluwer, Warszawa 2017.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Termin stabilność finansowa państwa jest używany zamiennie z pojęciem bezpieczeństwa finansowego państwa. Odwołując się do stanowiska A. Jurkowskiej-Zeidler należy się zgodzić, że bezpieczeństwo finansowe, rozumiane jako brak zewnętrznych i wewnętrznych zagrożeń gospodarczych, jest pojęciem nadrzędnym nad stabilnością finansową. Mianowicie stabilność finansowa jest bowiem metodologicznie przedmiotem ochrony bezpieczeństwa finansowego i rozumiana być może jako stan, w którym system finansowy działa bez zakłóceń, i w którym brak kryzysu finansowego i ryzyka systemowego[10].

Należy jednak zauważyć, iż pomimo zainteresowania tematyką stabilności finansowej termin ten pozostaje bez jednoznacznej definicji. Przegląd najpopularniejszych z nich przedstawia przeprowadziła K. Krzemińska oraz K. Górska pod nadzorem naukowym dr W. Tokarskiej-Ołowni i dr. R. Kowala.

Tabela 1. Zestawienie definicji pojęcia stabilności finansowej

Źródło	Definicja
O. Issing, *Monetary and Financial Stability: Is there a Trade-off?*, BIS, Conference on Monetary Stability, Financial Stability and the Business Cycle", 28–29 marca 2003, s. 1.	Stabilność finansowa to stan, w którym system finansowy jest zdolny w trwały sposób wypełniać swoje funkcje, tj. efektywnie alokować fundusze od oszczędzających do najbardziej produktywnych inwestorów
T. Padoa-Schioppa, *Central Banks and Financial Stability: Exploring the Land in between*, The Second ECB Central Banking Conference on the Transformation of the European Financial System", 24–25 października 2002, Frankfurt, s. 20.	Stabilność finansowa to stan, w którym system finansowy jest w stanie wytrzymać szoki bez tworzenia warunków do kumulowania się procesów, które w konsekwencji zakłócają alokację kapitału oraz przebieg płatności w gospodarce
J. Fidrmuc, F. Schardax, *Increasing Integration of Applicant Countries into International Financial Markets: Implications for Financial and Monetary Stability*, BIC Conference Papers, No. 8, Basle 2000, s. 92.	Stabilność finansowa to brak (nieobecność) kryzysów finansowych.
G.J. Schinasi, *Safeguarding Financial Stability, Theory and Practice*, International Monetary Fund, Washington 2005.	Stabilność finansowa ma miejsce, gdy system jest zdolny satysfakcjonująco wypełniać jednocześnie trzy swoje podstawowe funkcje: 1) efektywnie i sprawnie dokonywać alokacji środków od oszczędzających do inwestorów, 2) prawidłowo wyceniać ryzyko finansowe (również w perspektywie czasu) i relatywnie dobrze nim zarządzać, 3) łagodnie absorbować szoki realne i finansowe

[10] A. Jurkowska-Zeidler, *Bezpieczeństwo rynku finansowego w świetle prawa Unii Europejskiej*, a Wolters Kluwer business, Warszawa 2008. s. 166–171.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Zarządzanie wartością instytucji finansowej na integrującym się rynku finansowym – rola rady nadzorczej i zarządu, Gdańska Akademia Bankowa, Gdańsk, 27–28 maja 2003	Stabilność oznacza, że system finansowy jako całość nie wykazuje cech trwałej utraty płynności i/lub niewypłacalności, tj. instytucje finansowe są w stanie prowadzić nieprzerwaną działalność, a transakcje instrumentami finansowymi są realizowane w sposób ciągły
Przegląd stabilności systemu finansowego, I półrocze 2007 roku, Narodowy Bank Polski, 2007.	Stabilność systemu finansowego to stan, w którym system finansowy pełni wszystkie swoje funkcje w sposób ciągły i efektywny, nawet w przypadku wystąpienia nieoczekiwanych i niekorzystnych zaburzeń w znacznej skali
J.K. Solarz, *Międzynarodowy system finansowy. Analiza instytucjonalna – porównawcza*, Biblioteka Menedżera i Bankowca, Warszawa 2001, s. 183–184.	Stabilność finansowa to stan dynamicznej i trwałej równowagi na powiązanych ze sobą rynkach finansowych. Wyróżniamy: • stabilność bieżącą – wyznaczającą akceptowalny zakres zmian stanów na poszczególnych rynkach, • stabilność przyszłą (perspektywiczną) – odnoszącą się do braku istotnych słabości, mogącą uniemożliwić właściwą i terminową reakcję instytucji pośrednictwa finansowego na szoki asymetryczne.

Źródło: K. Krzemińska oraz K. Górska*, Pojęcie, znaczenie i istota stabilności systemu finansowego* (w:) *Стан та перспективи розвитку обліку, аналізу, контролю і оподаткування в умовах поглиблення євроінтеграційних процесів*, Сполом, Львів 2018, s. 33 i n.

Powyższe zestawienie definiowania pojęcia stabilność finansowa wskazuje na kilka wspólnych cech. Mianowicie wszystkie odwołują się do podstawowych funkcji systemu finansowego wobec gospodarki. Ponadto zauważalny jest związek pomiędzy sprawnością, z jaką je realizuje, a realną sferą gospodarki. Związek ten jest dwustronny – funkcjonowanie gospodarki realnej zależy od tego, jak sprawny jest system pośrednictwa finansowego, na kondycję systemu wpływa zaś stan gospodarki, która może być źródłem szoków zewnętrznych dla tego systemu. Dodatkowo warto pokreślić, że ww. zestawienie uwypukla fakt, iż stabilny system finansowy powinien być dynamiczny a nie statyczny (oderwany od „żywych procesów w obrocie gospodarczym"). Oczekuje się aby system finansowy państwa będzie się rozwijał i będzie jednocześnie stabilny. Takie rozumienie i takie podejście do stabilności finansowej państwa prowadzi wprost do pokreślenia roli i rangi regulacji AML w rozważanym zakresie[11].

[11] Pranie pieniędzy to złożone zjawisko. Przede wszystkim nie jest statyczne ani tymczasowe: nieustannie ewoluuje, pozyskując nowe zasoby w miarę postępującej globalizacji finansowej i roz-

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

W doktrynie przeważa pogląd, określający stabilność finansową w ujęciu dynamicznym. Stabilność finansowa państwa powinna być analizowana nie tylko w danym momencie, ale również przy uwzględnieniu przyszłych potencjalnych szoków zewnętrznie i wewnętrznie oddziałujących na odporności poszczególnych systemów i ostatecznie na odporności całego państwa[12].

Konieczne jest zauważenie, że przytoczone wyżej definicje mają również charakter systemowy, gdyż koncentrują się na odporności systemu finansowego jako całości i nie uznają upadku pojedynczego banku lub pojedynczego uczestnika rynku finansowego za dowód niestabilności finansowej państwa. Tu pojawia się kolejny obszar badań i szukanie odpowiedzi, czy destabilizacja jednego uczestnika rynku finansowego może zdestabilizować stabilność finansową państwa. Naturalnie wiele zależy od wielkości i skali potencjalnego uczestnika rynku. Radykalne zmiany cen aktywów, będące skutkiem realnych lub finansowych szoków i prowadzące do upadków pojedynczych instytucji finansowych, mogą nawet okazać się oznaką stabilności systemu finansowego, pod warunkiem że nie spowodują zachwiania zdolności całego systemu do efektywnego pośrednictwa finansowego i alokacji zasobów w państwie.

Mając na względzie dotychczasowe wyniki stan badań i analiz z zakresu funkcjonowania i organizacji systemu finansowego, utrzymanie stabilności systemu finansowego państwa należy rozpatrywać w następujących aspektach[13]:

- realizacji podstawowych funkcji systemu finansowego (można to także rozpatrywać pod kątem pojedynczego uczestnika, jego zadań statutowych i oczekiwań określonych przez normodawcę),
- zdolności do przezwyciężenia zewnętrznych szoków (posiadania przez konkretnego uczestnika buforów kapitałowych, sprawnych systemów przewidujących i zapobiegających niepożądanym zjawiskom),
- utrzymania zaufania do systemu finansowego (adekwatnie bank wobec klienta, państwo wobec podatnika i obywatela),
- dążenia do rozwoju gospodarczego przez promowanie produkcji i wzrostu gospodarczego (adekwatnie do zadań statutowych, przykładowo pożądane jest państwo, które w znacznej mierze wypracowywało PKB z inwestycji, a nie z konsumpcji, jak się dzieje aktualnie w Polsce).

woju technologicznego. Ma charakter ponadnarodowy, ponieważ nie tylko nie uznaje granic, ale wręcz wykorzystuje je do zacierania śladów powiązań między kolejnymi transakcjami finansowymi dokonywanymi na całym świecie i utrudniania działań wymiaru sprawiedliwości. Co więcej, jest to zjawisko przybierające na sile. Według szacunków Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (FATF) roczny wolumen operacji prania pieniędzy szacowany jest na 2 do 5% światowego PKB.

[12] O. Szczepańska, *Stabilność finansowa jako cel banku centralnego*, Wydawnictwo Naukowe Scholar, Warszawa 2008.

[13] A. Alińska, *Mechanizmy stabilności systemu finansowego*, C.H. Beck, Warszawa 2016, s. 48 i n.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Reasumując, istnieje powszechna zgoda, że stabilność systemu finansowego państwa stanowi fundamentalny warunek funkcjonowania gospodarki każdego kraju. Stabilność finansowa jest warunkiem koniecznym i niezbędnym do racjonalnych decyzji inwestora i podatnika o alokacji kapitału. To bezpośrednio sprzyja procesom inwestycyjnym i oszczędzaniu. Natomiast brak pewnego i bezpiecznego systemu finansowego w państwie daje niepewność i ryzyko zniechęcające do zawierania długookresowych umów oraz uniemożliwia właściwe funkcjonowanie instytucji finansowych.

1.3. DZIAŁANIA NBP NA RZECZ STABILNOŚCI KRAJOWEGO SYSTEMU FINANSOWEGO

Zgodnie z postanowieniami art. 3 ust. 2 pkt 6a i 6 ustawy o NBP[14], Narodowemu Bankowi Polskiemu powierzono ustawowe zadania działania na rzecz stabilności krajowego systemu finansowego oraz kształtowania warunków niezbędnych do rozwoju systemu bankowego. Ustawodawca przyjął ustalone w tradycji bankowości centralnej pryncypia, iż stabilność systemu finansowego jest bezpośrednim gwarantem a zarazem warunkiem:

- zrównoważonego wzrostu gospodarczego,
- stabilnego poziomu cen (podstawowym celem działalności NBP)[15].

Mając na względzie tematykę niniejszego rozdziału, jak i całej monografii, trzeba wskazać inną przesłankę działań NBP na rzecz stabilnego funkcjonowania systemu finansowego. Mianowicie zgodnie art. 3 pkt 2 ust. 1 ustawy o NBP bank centralny odpowiada za organizację rozliczeń pieniężnych. Sprawne działanie systemów płatniczych jest oparte na stabilnym funkcjonowaniu współtworzących je instytucji finansowych. Stąd wynika ranga i zakres udziału NBP w przeciwdziałaniu praniu pieniędzy.

Stabilność systemu finansowego oznacza, że cały system wypełnia prawidłowo swoje kluczowe funkcje przy realizacji strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu[16].

Szczególne znaczenie dla zachowania stabilności krajowego systemu finansowego ma utrzymanie stabilności sektora bankowego, gdyż odgrywa on kluczową rolę w finansowaniu gospodarki, transmisji impulsów polityki pieniężnej i rozliczeniach pieniężnych. Regulacje prawne dotyczące przeciwdziałania praniu pieniędzy

[14] Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (t.j. Dz.U. z 2020 r., poz. 2027).

[15] O. Szczepańska, *Stabilność finansowa jako cel banku centralnego. Studium teoretycznoporównawcze*, Scholar, Warszawa 2008.

[16] M. Torończak, *Komitet Stabilności Finansowej po zmianach*, „Monitor Prawa Bankowego" 2017, nr 5.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

oraz finansowaniu terroryzmu nałożyły szczegółowe obowiązki na szeroki katalog podmiotów, w tym na NBP. Bezpieczeństwo finansowe banków jest także szczególnie ważne z powodu pełnienia przez Narodowy Bank Polski funkcji pożyczkodawcy ostatniej instancji oraz współpracę z KNF i GIIF[17].

Narodowy Bank Polski analizuje i ocenia zagrożenia dla stabilności systemu finansowego. Wyniki analiz wraz z rekomendacjami działań ograniczających zidentyfikowane ryzyko są publikowane w Raporcie o stabilności systemu finansowego od 2001 r.[18]. Po wypracowaniu i przyjęciu ram prawnych Europejskiej Unii Bankowej identyfikacja, ocena i ograniczenie ryzyka systemowego są ważnymi elementami nadzoru makroostrożnościowego, w którego sprawowaniu wiodącą rolę odgrywają banki centralne UE (najściślej strefy euro)[19]. W celu przygotowania do realizacji zadań z tym związanych w NBP od 2011 r. funkcjonuje wewnętrzny Komitetu Ryzyka Systemowego.

NBP monitoruje i analizuje rozwój systemu finansowego w Polsce. Niedostateczny rozwój usług finansowych może hamować rozwój gospodarczy kraju, natomiast „przerost" systemu finansowego lub jego niewłaściwa struktura może być czynnikiem sprawczym lub zwiększającym zasięg i koszty kryzysu finansowego. NBP od 2001 r. w cyklicznie publikowanych raportach prezentuje wyniki analiz rozwoju usług finansowych w Polsce.

Narodowy Bank Polski odpowiadając za stabilności krajowego systemu finansowego i jego przyszłość współpracuje w szczególności z Ministerstwem Finansów, Komisją Nadzoru Finansowego oraz Bankowym Funduszem Gwarancyjnym. Przedstawiciele wskazanych instytucji wchodzą w skład Komitetu Stabilności Finansowej, którego zadaniem jest koordynacja działań na rzecz utrzymania lub przywrócenia stabilności systemu finansowego w przypadku bezpośredniego zagrożenia kryzysem i w czasie jego trwania.

Funkcje banku centralnego, ale również regulacje prawne dotyczące przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu są realizowane poprzez obecność NBP w wielu międzynarodowych organizacjach. NBP uczestniczy w pracach międzynarodowych instytucji działających na rzecz stabilności finansowej, a konkretnie w pracach Europejskiej Rady Ryzyka Systemowego.

Wcześniej zostało wskazane, że utrzymanie stabilności systemu finansowego kraju jest warunkiem sine qua non dla zrównoważonego wzrostu gospodarczego. Każdy z dostępnych raportów jednolicie wskazuje, że największy obrót odbywa się w formie bezgotówkowej i za pośrednictwem systemów bankowych. Uznając to

[17] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, red. A. Jurkowska-Zeidler, M. Olszak, Wolters Kluwer, Warszawa 2016.

[18] Raport o stabilności systemu finansowego jest publikowany w czerwcu oraz w grudniu każdego roku. Taki harmonogram publikacji pozwala na prezentację oceny sytuacji systemu finansowego w najczęściej wykorzystywanym przez analityków ujęciu, tj. w oparciu o dane finansowe na połowę i na koniec roku.

[19] A. Dobrzańska, *Polityka makroostrożnościowa banku centralnego*, Difin, Warszawa 2016.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

za pewnik, w sposób oczywisty to właśnie sektory bankowe i powiązane systemy rozliczeń są najbardziej narażone na spekulacje i łamanie przepisów dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Dlatego w centrum zainteresowania znajduje się kondycja sektora bankowego, gdyż odgrywa on kluczową rolę w krajowym systemie finansowym i w przestrzeganiu przepisów AML.

Funkcja płatnicza w ramach systemu finansowego ma zapewnić sprawny przepływ i dostęp do pieniądza z jednoczesnym respektowaniem ograniczeń AML. Zależy ona m.in. od bezpieczeństwa i efektywności działania systemu płatniczego nadzorowanego przez bank centralny, a jej zaburzenie może negatywnie wpływać na zaufanie do pieniądza i powodować powstawanie niepożądanych zjawisk np. terroryzmu (tradycyjnego i cyberterroryzmu). Wobec tego funkcje realizowane przez system finansowy można wiązać z funkcjami pełnionymi w gospodarce przez pieniądz (funkcja płatnicza, cyrkulacyjna, miernika wartości i tezauryzacyjną)[20].

1.4. WPŁYW I ZNACZENIE SYSTEMU AML NA STABILNOŚĆ FINANSOWĄ PAŃSTWA

Zgodnie z postanowieniami ustawy z dnia 18 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[21], system przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu tworzą:

- instytucje centralne,
- instytucje obowiązane,
- instytucje współpracujące.

Do instytucji centralnych (organy informacji finansowej) zaliczmy: Generalny Inspektor Informacji Finansowej, oraz minister właściwy do spraw instytucji finansowej. Ponadto cały system AML tworzą jednostki współpracujące, czyli organy administracji rządowej i samorządu terytorialnego, inne państwowe jednostki organizacyjne oraz Narodowy Bank Polski, Komisja Nadzoru Finansowego oraz Najwyższa Izba Kontroli[22].

Ważne funkcje w systemie AML pełnią podmioty, określane przez ustawodawcę jako instytucje obowiązane. W postanowieniach art. 2 ust. 1 ustawa z dnia 18 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terro-

[20] *Pieniądz i jego oddziaływanie na otocze*nie, red. P. Sitek, Warszawa 2016.

[21] T.j. Dz.U. z 2021 r., poz. 1132, 1163, 1535.

[22] M. Capiga, *Bezpieczeństwo instytucji finansowych jako instytucji obowiązanych w systemie przeciwdziałania praniu pieniędzy*, „Studia Ekonomiczne" 2014, nr 171, s. 120–131.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ryzmu został określony enumeratywnie katalog instytucji obowiązanych[23]. Zgodnie z obowiązującymi przepisami ustawy obowiązkiem instytucji obowiązanych jest prowadzenie bieżącego monitoringu stosunków gospodarczych, poprzez badanie transakcji, które są dokonywane w trakcie stosunków gospodarczych. Weryfikacja czy transakcje są zgodne z wiedzą instytucji obowiązanej na temat klienta oraz czy działalność i źródła pochodzenia środków, dokumentów oraz danych są na bieżąco uaktualniane. Jeżeli wystąpi sytuacja, że instytucja obowiązana nie będzie w stanie racjonalnie wyjaśnić działalności klienta, wówczas może to wskazywać na proceder prania pieniędzy lub finansowania terroryzmu. Poza analizą merytoryczną instytucje obowiązane mają za zadanie dokonać analizy formalnej, nakierunkowanej na badanie rzetelności danych oraz ich kompletności zawartych w rejestrze informacji o transakcjach[24]. Analiza powinna przede wszystkim podejmować identyfikację stron oraz wszelkie transakcje powinny być dokumentowane przez okres pięciu lat w formie pisemnej lub elektronicznej.

Poszczególne rozdziały niniejszej monografii podejmują szczegółowo określone zakresy ustawy z dnia 18 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Aby uniknąć powtórzeń, dalsze badania zostaną skierowane tylko na zagadnienia wspólne dla AML i stabilności finansowej państwa.

Walka z praniem pieniędzy i finansowaniem terroryzmu jest istotnym czynnikiem wpływającym na globalne bezpieczeństwo, a w szczególności integralności systemu finansowego i zrównoważonego wzrostu. Ustawodawca postępując w procesie legislacji tych źródeł prawa stara się eliminować i zapobiegać niewłaściwemu wykorzystywaniu rynku finansowego[25].

AML/CTF to pakiet legislacyjny dotyczący przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. W dniu 20 lipca 2021 r. Komisja Europejska przedstawiła ważny pakiet wniosków ustawodawczych, aby wzmocnić unijne przepisy dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Nowością jest propozycja zawarta w pakiecie, aby utworzyć nowy organ UE do walki z praniem pieniędzy. Wynika to z zobowiązania Komisji do ochrony obywateli UE i systemu finansowego UE przed praniem pieniędzy i finansowaniem terroryzmu. Celem głównym i bezpośrednim jest poprawa wykrywania podejrzanych transakcji i działań oraz zlikwidowanie luk wykorzystywanych przez przestępców do prania nielegalnych dochodów lub finansowania działalności terrorystycznej za pośrednictwem systemu finansowego.

[23] M.A. Kędzierski, *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce*, Wydawnictwo Adam Marszałek, Toruń 2019, s. 490.

[24] K. Grabowska, *MK Monitor księgowego wydanie specjalne: Przeciwdziałanie praniu brudnych pieniędzy oraz finansowaniu terroryzmu*, Inforlex, Warszawa 2019, s. 80.

[25] M. Lemmonier, *Europejskie modele instrumentów finansowych*, Wolters Kluwer, Warszawa 2017.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Aktualny pakiet AML/CFT składa się z czterech propozycji legislacyjnych:

- Rozporządzenie ustanawiające unijny organ ds. przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu[26] w formie zdecentralizowanej agencji regulacyjnej UE,
- nowe rozporządzenie w sprawie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu[27], zawierające bezpośrednio stosowane przepisy dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w tym zmieniony unijny wykaz podmiotów podlegających przepisom dotyczącym przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (tzw. podmioty zobowiązane),
- Dyrektywa w sprawie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, zastępująca dotychczasową unijną dyrektywę w sprawie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (dyrektywa 2015/849 ze zmianami[28]) i zawierająca przepisy nieodpowiednie dla rozporządzenia i wymagające transpozycji na szczeblu krajowym, takie jak przepisy dotyczące krajowych organów nadzoru i jednostek analityki finansowej w państwa członkowskie,
- przekształcenie rozporządzenia z 2015 r. w sprawie transferów środków finansowych (rozporządzenie 2015/847).

Powyższe cztery propozycje stanowią ważny zestaw środków służących modernizacji unijnego systemu AML/CFT[29]. Podejmowane próby legislacyjne UE zmierzają do ustanowienie zintegrowanego, nowszego, solidniejszego, a przede wszystkim odpowiadającego na aktualne zagrożenia Pakiety AML.

Powstaje uzasadnione pytanie problemowe, dlaczego ten Pakiet AML jest tak ważny z punktu widzenia stabilności finansowej? Na wszystkich poziomach władzy publicznej i korporacyjnej jest zgoda, że pranie pieniędzy i finansowanie terroryzmu (ML/TF)[30] stanowią poważne zagrożenie dla integralności gospodarki i systemu finansowego UE oraz dla bezpieczeństwa krajów członkowskich i ich obywateli.

[26] Komisja Europejska, Remarks by Executive Vice-President Dombrovskis at the ECOFIN press conference, ec.europa.eu/commission/presscorner/detail/en/speech_21_4673 (data dostepu: 2 września 2021).

[27] Komisja Europejska, Press material from the Commission Spokesperson's Service, ec.europa.eu/commission/presscorner/home/en#_ftn2 (data dostępu: 2 września 2021).

[28] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.

[29] AML/CTF – Przeciwdziałanie praniu pieniędzy i przeciwdziałanie finansowaniu terroryzmu.

[30] ML/FT – Pranie pieniędzy i finansowanie terroryzmu.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Według szacunku Europolu około 1% rocznego produktu krajowego brutto UE dotyczy podejrzanej działalności finansowej[31]. W następstwie wielu głośnych przypadków prania pieniędzy w UE w 2019 r. komisja przyjęła komunikat w sprawie lepszego wdrażania unijnych ram przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oraz cztery sprawozdania dotyczące różnych aspektów polityki przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Przeanalizowano skuteczność i wydajność obecnego unijnego systemu przeciwdziałania praniu pieniędzy/finansowaniu terroryzmu (AML/CFT) i wyciągnięto wnioski o potrzebie pilnych reformy odpowiadających zidentyfikowanym zagrożeniom.

W dniu 7 maja 2020 r. komisja przedstawiła plan działania dotyczący kompleksowej polityki Unii w zakresie zapobiegania praniu pieniędzy i finansowaniu terroryzmu. Plan działania określa środki prawne, które komisja będzie podejmować dla lepszego egzekwowania, nadzorowania i koordynowania przepisów UE w tej dziedzinie. KE m.in. zamierzała: zapewnić skuteczne wdrożenie istniejących unijnych ram AML/CFT, ustanowienie jednolitego zbioru przepisów UE w zakresie AML/CTF, wprowadzenie nadzoru AML/CFT na poziomie UE, ustanowienie mechanizmu wsparcia i współpracy dla FIUs[32], egzekwowanie przepisów prawa karnego na szczeblu UE i wymianę informacji.

W 2020 r. na poziomie organów unijnych uznano, że obecne ramy AML/CFT w formie dyrektywy w praktyce wywodują perturbacje w procesie transpozycji do prawa krajowego. Skutkuje to opóźnieniami we wdrażaniu, a dodatkowo prowadzi do rozbieżności w przepisach krajowych. Nie sprzyja to walce z AML/CFT, lecz prowadzi do fragmentarycznego uregulowania w różnych krajach UE, co jest wykorzystywane w zjawisku prania pieniędzy. Mimo niechęci do powstawania nowych form administracji i nowego zatrudnienia w UE zauważalny jest brak jest centralnego organu koordynującego na szczeblu UE. Brak centralnego organu, wyposażonego w kompetencje i zadania, utrudnia a wręcz uniemożliwia współpracę między krajowymi organami nadzoru i jednostkami analityki finansowej (FIU).

Nowy unijny urząd ds. przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AMLA – organ UE ds. przeciwdziałania praniu pieniędzy) będzie miał dwa główne obszary działalności: nadzór AML/CFT oraz wspieranie jednostek analityki finansowej UE (FIU). W praktyce oczekuje się, że AMLA stanie się centrum zintegrowanego systemu krajowych organów nadzoru AML/CFT, zapewniając ich wzajemne wsparcie i współpracę. Celem jest konwergencja nadzoru i wspólne standardy nadzoru. Urząd będzie pełnił rolę koordynacyjną w sektorze niefinansowym. W sektorze finansowym będzie również bezpośrednio nadzorował podmioty

[31] COM(2021) 422 fina. Proposal for a Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-assets (Recast).

[32] FIU – jednostki analityki finansowej.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

sektora finansowego, które są narażone na największe ryzyko prania pieniędzy i finansowania terroryzmu.

Nowy urząd ma powstać w 2023 r. w celu rozpoczęcia większości działań w 2024 r. Ostatecznie pełny stan zatrudnienia ma osiągnąć w 2026 r. i w całkowitym zakresie rozpocząć bezpośredni nadzór nad niektórymi podmiotami finansowymi wysokiego ryzyka. Jednakże należy zwrócić uwagę, że bezpośredni nadzór może rozpocząć się dopiero po wejściu w życie zharmonizowanego zbioru przepisów.

Kolejna wątpliwość dotyczy status quo krajowych organów nadzoru i jednostek analityki finansowej po wdrożeniu unijnego urzędu ds. przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AMLA), czy zostaną zniesione i zastąpione przez nowy organ UE? Unijny ustawodawca planuje, aby krajowe organy nadzoru i jednostki analityki finansowej dalej pozostawały kluczowym elementem unijnego systemu egzekwowania przepisów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Nowy urząd UE zastąpi krajowe organy nadzoru jedynie jako organ nadzoru niewielkiej liczby transgranicznych podmiotów sektora finansowego w najwyższej kategorii ryzyka. Warto zauważyć, iż nowy pakiet tworzy zintegrowany system nadzoru UE w zakresie przeciwdziałania praniu pieniędzy, bezpośrednio angażujący krajowe organy nadzoru i Urząd UE ds. AML. Urząd będzie również odgrywał kluczową rolę we wspieraniu krajowych FIU w prowadzeniu wspólnych analiz, ale sam nie będzie miał status quo FIU i nie zastąpi krajowych FIU.

Nowy urząd UE ds. AML będzie nadzorował bezpośrednio instytucje finansowe na dwa sposoby:

- podmioty zobowiązane z sektora finansowego, które prowadzą działalność w znacznej części państw członkowskich i mają najwyższy profil ryzyka w kilku z tych państw członkowskich, zostaną wybrane do bieżącego bezpośredniego nadzoru ze strony urzędu. Wybór ten będzie oparty na obiektywnych kryteriach skoncentrowanych na kategoryzacji ryzyka i działalności transgranicznej. Lista będzie weryfikowana okresowo co trzy lata. Aby zapewnić równy i sprawiedliwy wybór, metodyka kategoryzacji ryzyka podmiotów przez krajowe organy nadzoru zostanie ujednolicona przed pierwszym wyborem. Pierwszy proces selekcji oparty na zharmonizowanej metodologii zostanie przeprowadzony przez AMLA w 2025 r., a wybrane podmioty przejdą pod nadzór na szczeblu UE od 2026 r.,
- urząd będzie mógł wystąpić z wnioskiem o decyzję komisji w sprawie objęcia podmiotu zobowiązanego z sektora finansowego jego bezpośrednim nadzorem, niezależnie od kryteriów. Taka sytuacja może mieć miejsce, jeśli istnieją przesłanki wskazujące, że podmiot systematycznie nie spełnia swoich wymogów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oraz że istotne ryzyko prania pieniędzy lub finansowania terroryzmu może się urzeczywistnić, jeżeli krajowy organ nadzoru nie będzie w stanie podjąć szybkich

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

i skutecznych działań w celu radzenia sobie z takimi rodzajami ryzyka, jak: zalecane przez urząd.

Warto zauważyć, że nadzór nad ww. podmiotami bezpośrednio będzie wykonywany przez wspólne zespoły nadzorcze kierowane przez pracowników urzędu, w skład których mają wchodzić pracownicy krajowych organów nadzoru. Model ten został zaczerpnięty z metod pracy Jednolitego Mechanizmu Nadzorczego UE dla nadzoru ostrożnościowego nad bankami[33].

Jednolity zbiór przepisów UE dotyczący przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu odnosi się do ujednoliconych ram regulacyjnych dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, które obejmują bezpośrednio obowiązujące zasady i wymogi dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu nałożone na podmioty zobowiązane. Przepisy te nie będą już wymagały transpozycji do prawa krajowego. Zasady na poziomie UE będą bardziej szczegółowe niż obecnie i będą obejmować wiele regulacyjnych standardów technicznych, które zostaną przygotowane przez przyszły organ UE ds. przeciwdziałania praniu pieniędzy (na przykład w sprawie należytej staranności wobec klienta). Państwa członkowskie nadal będą mogły reagować na określone rodzaje ryzyka, na przykład wymagając od dodatkowych sektorów na szczeblu krajowym stosowania przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, jeśli jest to uzasadnione konkretnymi rodzajami ryzyka w danym państwie członkowskim.

Z punktu widzenia konieczności zapewnienia stabilności finansowej państwa newralgiczną kwestią jest lista „podmiotów zobowiązanych". Podmioty zobowiązane do stosowania rygorów AML/CFT, w tym do przeprowadzania należytej staranności wobec klientów oraz, w przypadku podejrzeń, do zgłaszania tych podejrzeń FIU. Aktualnie prawie wszystkie instytucje finansowe to podmioty zobowiązane (banki, zakłady ubezpieczeń na życie, dostawcy usług płatniczych i firmy inwestycyjne) oraz różnego rodzaju podmioty i podmioty niefinansowe, w tym prawnicy, księgowi, pośrednicy w obrocie nieruchomościami, kasyna i niektóre rodzaje kryptowalut. Ponadto dostawcy usług związanych z aktywami.

Nowy pakiet AML w dużej mierze wprowadza regulacje dotyczące właściwości rzeczywistej i rejestrów. Właściwość rzeczywista została wprowadzona dyrektywą (UE) 2015/849 w celu zwiększenia przejrzystości złożonych struktur korporacyjnych. Beneficjent rzeczywisty to każda osoba fizyczna, która ostatecznie jest właścicielem lub kontroluje podmiot prawny, lub podobną umowę prawną. Przepisy dotyczące informacji o beneficjentach rzeczywistych zawarte w rozporządzeniu wyjaśniają i rozszerzają przepisy obowiązujące w obecnym prawodawstwie UE w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w tym

[33] Szerzej na temat jednolitego mechanizmu nadzorczego: P. Sitek, *Zintegrowany sektor bankowy Unii Europejskiej. Studium prawno-finansowe*, Vizja Press & IT, Warszawa 2015.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

pojęcie beneficjenta rzeczywistego oraz wymóg, aby wszystkie podmioty korporacyjne i inne podmioty prawne uzyskiwały i posiadały odpowiednie, dokładne i aktualne informacje o beneficjentach rzeczywistych.

Propozycje nowego pakietu AML zawierają bardziej precyzyjne i zharmonizowane regulacje. Nowe przepisy wyjaśniają także wymóg zgłaszania tych informacji do krajowych rejestrów beneficjentów rzeczywistych. Nowością jest obowiązek rejestrowania przez podmioty prawne spoza UE, które są powiązane z UE, ich beneficjentów rzeczywistych w unijnych rejestrach beneficjentów rzeczywistych. Ustawodawca unijny dąży do zwiększenia adekwatności, dokładności i aktualności danych o beneficjentach rzeczywistych dostępnych w rejestrach dzięki zharmonizowanym przepisom. Ponadto podmioty odpowiedzialne za krajowy rejestr beneficjentów rzeczywistych otrzymają więcej uprawnień w celu weryfikacji.

Bezpośrednio dążąc do stabilności systemu finansowego, nowy pakiet AML pójdzie dalej w sprawie gromadzenia informacji o rachunku bankowym. Mianowicie komisja proponuje utworzenie transgranicznego systemu między tymi krajowymi rejestrami lub mechanizmami, aby umożliwić FIU również dostęp do informacji z innych państw członkowskich. Jest to skutek przeprowadzenia szerokich konsultacji przeprowadzonych w pakiecie AML w lipcu 2019 r. Proponowana zmiana dyrektywy w sprawie dostępu do informacji finansowych zapewni organom ścigania również dostęp i przeszukiwanie systemu łączącego rejestry rachunków bankowych. Umożliwi to organom ścigania szybkie ustalenie, czy podejrzany posiada rachunki bankowe w innych państwach członkowskich, a tym samym ułatwi prowadzenie dochodzeń finansowych i odzyskiwanie mienia w sprawach transgranicznych. Wszystkie solidne zabezpieczenia zawarte w dyrektywie w sprawie dostępu do informacji finansowych będą miały również zastosowanie do dostępu organów ścigania do informacji o rachunku bankowym.

Kolejną ważną kwestią są planowane zmiany w sprawie transferów środków. Proponowana jest zmiana rozporządzenia UE z 2015 r. w sprawie transferów środków pieniężnych (rozporządzenie 2015/847), aby rozszerzyć jego zakres na transfery kryptowalut. Oznacza to, że pełne informacje o nadawcy i odbiorcy takich przelewów będą musiały być zawarte przez dostawców usług związanych z kryptowalutami we wszystkich transferach wirtualnych aktywów, tak jak obecnie robią to dostawcy usług płatniczych w przypadku przelewów bankowych. Uzasadnienie wynika z konieczności identyfikowania tych, którzy wysyłają i odbierają aktywa kryptograficzne do celów przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, identyfikowanie ewentualnych podejrzanych transakcji i w razie potrzeby blokowanie ich. Niestety, ale zjawisko „proceder" kryptowalut są coraz częściej wykorzystywane do prania pieniędzy i innych celów przestępczych. Dlatego pilne i konieczne jest zaktualizowanie ram prawnych UE i przyjęcie rozporządzenia w sprawie rynków aktywów kryptograficznych (MiCA), które określi wymogi dla unijnych emitentów aktywów kryptograficznych i dostawców usług związanych

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

z kryptowalutami, w procedurze ubiegania się o zezwolenie na świadczenie swoich usług na jednolitym rynku.

Komisja proponuje również zobowiązanie wszystkich dostawców usług w zakresie aktywów kryptograficznych zaangażowanych w transfery aktywów kryptograficznych do gromadzenia i udostępniania danych dotyczących inicjatorów i beneficjentów transferów aktywów wirtualnych lub kryptograficznych, które prowadzą. Nastąpi to poprzez zmianę rozporządzenia z 2015 r. w sprawie transferów środków[34].

Stabilność finansowa państwa opiera się na rosnącej liczbie transakcji bezgotówkowych i rosnącej nieustannie potrzebie identyfikacji cyfrowej uczestnika rynku finansowego. Dlatego komisja widzi potrzebę wzmacniania zdalnej identyfikacji. Rozwiązania dotyczące tożsamości cyfrowej są niezbędne dla obywateli i przedsiębiorstw, aby zapewnić bezpieczny dostęp do usług cyfrowych. Stanowią one kluczowy krok w kierunku cyfryzacji finansów i łatwiejszego wykorzystania potencjału rynku wewnętrznego. Jak wynika ze strategii finansów cyfrowych, Komisja Europejska pracuje nad ustanowieniem nowych ram prawnych dla interoperacyjnego korzystania z rozwiązań tożsamości cyfrowej. Wymusza to konieczność wprowadzenia ram prawnych, umożliwiających bezpieczne, lecz zdalne wprowadzanie klientów na rynek finansowy w całej UE. Propozycje dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu doprecyzowują, za pomocą standardów technicznych, aspekty związane ze szczegółową identyfikacją i elementami uwierzytelniania do celów onboardingu. Warto zauważyć, iż zmiany w ramach AML/CFT będą bezproblemowo współdziałać z proponowanymi przez komisję ramami Europejskiej Tożsamości Cyfrowej, tak ułatwiać przeprowadzanie transakcji z jednoczesnym eliminowaniem zjawisk niepożądanych.

Transakcje gotówkowe z punktu widzenia statystyk płynących z rynku finansowego stają się coraz rzadsze. Jednakże to właśnie transakcje gotówkowe są najtrudniejsze w monitorowaniu, stąd pozostają w spektrum zainteresowania grup przestępczych. Transakcje i zakupy gotówkowe pozwalają na inwestowanie nielegalnych dochodów w realną gospodarkę. Obecne przepisy UE już uwzględniają ryzyko i wymagają od wszystkich operatorów handlujących towarami, które otrzymują płatności gotówkowe powyżej 10 000 EUR, stosowania wymogów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Natomiast państwa członkowskie mogą przyjąć bardziej rygorystycznych pułapy.

Komisja proponuje wprowadzenie jednolicie w UE maksymalnej kwoty 10 000 euro dla dużych transakcji gotówkowych, a państwa członkowskie będą mogły na szczeblu krajowym ustalać niższe limity. Taka górna granica będzie miała znaczący wpływ na ograniczenie prania pieniędzy i finansowania terro-

[34] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781, 2006.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ryzmu w UE, przy jednoczesnym utrzymaniu statusu euro jako prawnego środka płatniczego. Proponuje się mechanizmy zapewniające, że taki środek nie wyklucza obywateli z systemu finansowego.

Komisja w nowym pakiecie AML proponuje zmienione podejście do zagrożeń płynących z państw trzecich. Chodzi o zapewnienie szybkiego i jednolitego w ramach UE identyfikowania zewnętrznych zagrożeń dla systemu finansowego Unii.

1.5. PODSUMOWANIE

Za stabilność finansową w Polsce odpowiedzialne jest: MF, NBP, KNF i ich szefowie (KSF) oraz BFG i GIIF. Poza ww. siatką bezpieczeństwa finansowego odpowiedzialnego za należyte działanie systemu bankowego i jego stabilności funkcjonuje NIK[35]. Wskazane wyżej instytucje państwa nadzorujące lub koordynujące rynkiem finansowym są na ogół centralnymi organami administracji państwowej działającymi w oparciu o przepisy ustawy. Tworzą system, który powinien zapewnić prawidłowe funkcjonowanie tego rynku, jego stabilność, bezpieczeństwo[36], przejrzystość oraz zaufanie do rynku finansowego.

Prawidłowe funkcjonowanie rynku finansowego w kraju, jak i stabilność finansowa państwa jest narażone na pranie pieniędzy, które to zjawisko stanowi jeden z najpoważniejszych destabilizujących czynników.

Założony na wstępie cel rozdziału został osiągnięty w pełni. Podkreślenia wymaga fakt, że przedmiotowa problematyka ma charakter interdyscyplinarny i dotyczy bardzo dynamicznie zmieniających się problemów naukowych. Przeprowadzono szczegółową analizę pojęcia stabilności finansowej tak w odniesieniu do rynku finansowego, jak również w połączeniu ze stabilnością finansową państwa. W szczególności zostały przybliżone komponenty pojęcia stabilności finansowej i wielopłaszczyznowości jego rozumienia oraz wskazanie na możliwe źródła jego ujęcia, a przez to również przybliżenie zmiany układu sieci stabilności finansowej w architekturze finansowej UE przez zmianę akcentu normatywnego w poszczególnych elementach tej sieci[37]. Jednocześnie przeanalizowano rolę przepisów doty-

[35] S. Szydło, *Problemy stabilizacji polskiej gospodarki w okresie rynkowych reform*, Wydawnictwo Naukowe AGH, Kraków 2013, s. 27.

[36] M.A. Kędzierski, *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22 (12), s. 120–142.

[37] P. Sitek, *Przeobrażenia systemu bankowego w kontekście utworzenia unii bankowej*, Wolters Kluwer, Warszawa 2017, s. 253–269.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

czących przeciwdziałania praniu pieniędzy i zwalczania terroryzmu w związku z koniecznością zapewnienia stabilności finansowej państwa.

W szczególności AMLA:

- ustanowi jednolity zintegrowany system nadzoru AML/CFT w całej UE, oparty na wspólnych metodach nadzorczych i konwergencji wysokich standardów nadzorczych,
- zapewni bezpośredni nadzór nad najbardziej ryzykownymi instytucjami finansowymi, które działają w wielu państwach członkowskich lub wymogą natychmiastowe działania w celu przeciwdziałania nieuchronnemu zagrożeniu dla stabilności finansowej,
- zapewni monitorowanie i koordynację pomiędzy krajowymi organami nadzoru odpowiedzialnymi za inne podmioty finansowe, a także koordynację organów nadzoru wobec podmiotów niefinansowych,
- będzie wspierać współpracę między krajowymi jednostkami analityki finansowej oraz ułatwiać koordynację i wspólne analizy między nimi, aby lepiej wykrywać nielegalne przepływy finansowe o charakterze transgranicznym[38].

Jednolity zbiór przepisów UE dotyczący przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu zharmonizuje przepisy dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w całej UE, w tym na przykład bardziej szczegółowe przepisy dotyczące należytej staranności wobec klienta, właściwości rzeczywistej oraz uprawnień i zadań organów nadzoru i jednostek analityki finansowej (FIU). Istniejące krajowe rejestry rachunków bankowych zostaną połączone, zapewniając szybszy dostęp dla usług rynku finansowego.

Reasumując Komisja Europejska przedstawiła ambitny pakiet ustawodawczy, mający na celu wzmocnienie unijnych przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT). Pakiet zawiera również propozycję utworzenia nowego organu UE do walki z praniem pieniędzy. Celem jest usprawnienie wykrywania podejrzanych transakcji i działań oraz zamknięcie luk wykorzystywanych przez przestępców do prania nielegalnych dochodów lub finansowania działalności terrorystycznej za pośrednictwem systemu finansowego w tym również destabilizacja systemu finansowego pojedynczego państwa, jak i całej UE. Jak przypomniano w strategii UE na rzecz bezpieczeństwa Unii na lata 2020–2025, wzmocnienie ram UE w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu pomoże również chronić Europejczyków przed terroryzmem i przestępczością zorganizowaną. Konieczne jest utrzymanie wysokiego tempa identyfikacji zmian w otoczeniu finansowym i ryzyka nowych zagrożeń dla stabilności finansowej kraju i całej UE. Nowe wyzwania związane z innowacjami technologicznymi charakteryzują się wielką dynamiką i nie mogą pozostać zlekce-

[38] Notaries of Europe Providing legal certainty, *Zwalczanie prania pieniedzy. walka globalna, wyzwanie dla Europy*, nr 2, maj 2020.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ważone. Warto przypomnieć waluty wirtualne, bardziej zintegrowane przepływy finansowe na jednolitym rynku oraz globalny charakter organizacji terrorystycznych, które wyraźnie wykorzystują cyberprzestrzeń do cyberprzestępczości.

Wiadomym jest, iż omawiane zjawisko określa czynności, których celem jest ukrycie pochodzenia środków finansowych uzyskanych z działalności przestępczej oraz nadania im cech charakterystycznych dla legalnych dochodów. Pranie pieniędzy znacząco wpływa na destabilizację gospodarki, zakłóceń w systemie podatkowym oraz walutowym poszczególnych państw. Proceder ten znacząco narusza zasady uczciwej konkurencji, a także powoduje dysproporcję mechanizmu rynkowego określania parametrów ekonomicznych. Pranie pieniędzy wpływa na korupcję w organach administracji, szczególnie w przypadkach jednostek decyzyjnych w zakresie zakazów odnoszących się do niektórych obszarów działalności gospodarczej. Wiadomym jest, iż poprzez zjawisko omawianego przestępstwa przejmowane są niektóre sektory gospodarki przez grupy przestępcze o charakterze zorganizowanym. Do innych zagrożeń płynących z tego rodzaju nadużyć należy wykorzystywanie działalności instytucji finansowych, co w rezultacie prowadzi do zachwiania stabilności finansowej, jak również strat innych podmiotów. Proceder zasadniczo wpływa na korumpowanie pracowników instytucji dokonującej podejrzanego rodzaju transakcji, co w konsekwencji powoduje zwiększenie strat poprzez nieuzasadnione ekonomicznie decyzje oraz nadużycia.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Izabela Juhnke
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 2.

MLRO – *MONEY LAUNDERING REPORTING OFFICER* – OSOBISTA ODPOWIEDZIALNOŚĆ CZŁONKÓW ZARZĄDU WEDŁUG USTAWY AML/CFT

2.1. UWAGI WPROWADZAJĄCE

Kształt polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu wyznaczają przede wszystkim przepisy prawne, zarówno krajowe, jak i Unii Europejskiej. Podstawowym aktem prawnym w tym obszarze jest ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[1]. Niemniej stale rozwijające się przepisy, zasady, rekomendacje i polityka w obszarze biznesu pozwoliły na wykształcenie procedur zgodnościowych, a tym samym stanowiska *Compliance Officer* (OC), czyli oficera ds. zgodności, którego zadaniem jest wdrożenie tych zasad i ich bieżące przestrzeganie[2]. Stosownie do uzyskanych doświadczeń wykreowano specjalistyczną i kierunkową politykę zgodnościową w obszarze AML/CFT. Skutkiem tego stało się stworzenie stanowiska *Anti-Money Laudering Compliance Officer* (AMCLO), czyli oficera ds. zgodności z ustawą o przeciwdziałaniu praniu pieniędzy, zgodnie z art. 8 u.p.p.p.f.t., który nakazuje instytucjom obowiązanym wskazanie pracownika, zajmującego kierownicze stanowisko, którego zadaniem będzie zapewnienie zgodności działalności tej instytucji, jak i jej pracowników z przepisami ustawy. Taki pracownik będzie nosił

[1] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. z 2021 r., 1132 t.j. z dnia 24 czerwca 2021 r., zwana dalej u.p.p.p.f.t.

[2] M.A. Kędzierski, *Obowiązki i odpowiedzialność oficera AML (AMLO) w instytucji obowiązanej, cz. 1,* „Prokuratura i Prawo" 2021, nr 5, s. 66–91.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

miano *Anti-Money Laudering Officer* (AMLO). Oprócz wskazanych obowiązków konieczne jest także raportowanie transakcji, a osobą za to odpowiedzialną będzie *Money Laundering Reporting Officer* (MLRO). Należy zaznaczyć, iż polski ustawodawca nie sugerował się zapisem IVDAML[3] w zakresie wskazówki, że osoba ta (AMLO) powinna być wyznaczona jedynie w sytuacji, gdy „jest to stosowne z uwagi na wielkość i charakter działalności" instytucji obowiązanej, a co za tym idzie, nakazał bezwzględne jej wyznaczenie. Wart uwagi jest również art. 154 u.p.p.p.f.t., który określa odpowiedzialność za delikt administracyjny związany z niezrealizowaniem wspomnianych obowiązków. Mniej istotne jest, czy pracownik AMLO będzie realizował czynności osobiście, czy w zespole, oraz w jaki sposób będzie wykonywany nadzór i kontrola w tym zakresie, jednak przepisy wewnętrzne funkcjonujące w tym obszarze, bezwzględnie powinny uwzględniać obowiązki, które wynikają z u.p.p.p.f.t. Przepisy te również nie mogą pozostawać w sprzeczności z rozwiązaniami systemowymi w obszarze AML/CFT, a tym samym powinny zapewniać kompleksową ochronę instytucji obowiązanej[4].

2.2. POWOŁANIE AMLO, MLRO

Do podstaw prawnych powołania MLRO należy zaliczyć: rekomendacje *Financial Action Task Force* (FATF), czyli Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy, która zajmuje się kreowaniem i promowaniem skutecznych rozwiązań prawnych, regulacyjnych i operacyjnych. Celem tych rozwiązań jest przeciwdziałanie praniu pieniędzy, finansowaniu terroryzmu oraz innym powiązanym zagrożeniom, skierowanym przeciwko integralności międzynarodowego systemu finansowego. Rekomendacje te tworzą pełny i spójny zespół środków, który powinien zostać implementowany przez poszczególne kraje. W treści zaleceń wzięto pod uwagę regulacje konwencji wiedeńskiej z 1988 r., a także zalecenia Bazylejskiego Komitetu Nadzoru Bankowego[5]. Co prawda Polska nie jest bezpośrednio członkiem FATF, jednak istotne jest, że uczestniczy w pracach tejże instytucji za pośrednictwem MONEYVAL, tj. Komitetu Ekspertów ds. Oceny Systemów Zwalczania Procederu Prania Pieniędzy i Finansowania Terroryzmu[6]. Zalecenia FATF wielo-

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE, zwana dalej: IVDAML.

[4] *Ibidem.*

[5] P. Siejczuk, *Problematyka prania brudnych pieniędzy w regulacjach prawnomiędzynarodowych, europejskich i krajowych*, http://www.bbn.gov.pl/ (data dostępu: 21.08.2021).

[6] *Systemy zarządzania zgodnością. Compliance w praktyce*, red. B. Jagura, B. Makowicz, Wolters Kluwer, Warszawa 2020.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

krotnie wskazują na zgodność działań instytucji z przestrzeganiem zasad, rekomendacji i międzynarodowych standardów, które związane są z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu. Regulacje dotyczą rodzajów instytucji oraz świadczonych usług. I choć obszar zgodności nie jest przedstawiony wprost to obowiązki tego typu należy wyłonić z kilku rekomendacji. Tym samym zgodnie z rekomendacją 14, zobowiązano kraje do zapewnienia zgodności, o których mówią Rekomendacje FATF dla osób fizycznych i prawnych, zajmujące się usługami transferu środków pieniężnych bądź innych wartości majątkowych. Rekomendacja 17 zleca osobom trzecim wykonywanie obowiązków badania klienta, zaś 18 zobowiązuje instytucje finansowe do wprowadzenia programów przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Natomiast nadzór nad tego typu instytucjami, jak i monitorowanie zgodności regulują rekomendacje 26 i 27. Zasady nakładania kar za naruszenie obowiązków zgodności z Rekomendacjami zostały uregulowane w rekomendacji 35[7]. Należy również zwrócić uwagę na notę interpretacyjną do zalecenia 18, która nakreśla, iż programy instytucji finansowych przeciwko praniu pieniędzy i finansowaniu terroryzmu powinny obejmować opracowanie wewnętrznych zasad, procedur i kontroli, w tym odpowiednich rozwiązań w zakresie zarządzania zgodnością oraz odpowiednich procedur sprawdzających w celu zapewnienia wysokich standardów przy zatrudnianiu pracowników. Rozwiązania dotyczące zarządzania zgodnością powinny obejmować powołanie inspektora zgodności na poziomie zarządzania[8].

Wspomniana już wcześniej Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (IVDAML) jest kolejnym aktem prawnym zawierającym wytyczne związane z wprowadzeniem standardów zgodnościowych oraz przepisy, które dotyczą osób odpowiedzialnych za ich powstanie, monitoring i wdrożenie[9]. Dyrektywa ta ma na celu zwalczanie prania pieniędzy oraz finansowania terroryzmu poprzez zapobieganie wykorzystaniu rynku finansowego do tych celów. Rozszerza ona zakres stosowania dotychczas obowiązującej dyrektywy (WE) 2005/60 (tj. trzeciej dyrektywy w sprawie przeciwdziałania praniu pieniędzy), która weszła w życie w 2007 r., a także ją zastępuje. Tym samym zmienia także rozporządzenie Parlamentu Europejskiego

[7] *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz Proliferacji Rekomendacje FATF*, Urząd Komisji Nadzoru Finansowego. Przetłumaczył: R. Obczyński (Departament Inspekcji Bankowych i Instytucji Płatniczych, Wydział Przeciwdziałania Praniu Pieniędzy), https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacje_FATF_40223.pdf (data dostępu: 19.08.2021).

[8] Recommendation 18: Internal controls and foreign branches and subsidiaries, https://cfatf-gafic.org/index.php/documents/fatf-40r/384-fatf-recommendation-18-internal-controls-and-foreign-branches-and-subsidiaries (data dostępu: 19 sierpnia 2021).

[9] M.A. Kędzierski, *Obowiązki i odpowiedzialność oficera AML (AMLO) w instytucji obowiązanej, cz. 1…*

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

i Rady (UE) nr 648/2012. Jej celem jest również wyeliminowanie wszelkich dwuznacznych przepisów dotychczasowej dyrektywy i powiązanych z nią aktów prawnych, a także zwiększenie spójności uregulowań dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu we wszystkich państwach UE. W czwartej dyrektywie w sprawie przeciwdziałania praniu pieniędzy uwzględniono zalecenia FATF z 2012 r.[10]. Podstawą do powołania Oficera AML według tej dyrektywy jest art. 8 ust. 3 i 4 pkt a, gdzie wskazano, iż państwa członkowskie zapewniają posiadanie przez podmioty zobowiązane (tj. w polskim systemie prawnym instytucje obowiązane) strategii, środków kontroli oraz procedur służących skutecznemu ograniczaniu ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu oraz skutecznemu zarządzaniu tym ryzykiem zidentyfikowanym na poziomie Unii, państwa członkowskiego oraz na poziomie instytucji obowiązanej. Tym samym, aby zapewnić realizację wspomnianych działań, instytucja obowiązana, o ile jest to stosowne z uwagi na wielkość i charakter jej działalności, zobowiązana jest do wyznaczenia pracownika odpowiedzialnego za zapewnienie zgodności z odpowiednimi przepisami na szczeblu kadry kierowniczej oraz kontrole pracowników. Jak już wcześniej wskazano, art. 8 u.p.p.p.f.t. stanowi transpozycję art. 8 ust. 4 pkt a IV dyrektywy AML z tą różnicą, że według polskiego prawodawcy bezwzględnie należy wyznaczyć takowego pracownika w przeciwieństwie do wskazówek IVDAML, gdzie osoba ta wyznaczana jest jedynie w sytuacji, gdy „jest to stosowne z uwagi na wielkość i charakter działalności”[11]. Jednocześnie dyrektywa ta w art. 33 ust. 2 nakłada na tę osobę zobowiązania do przekazania informacji z własnej inicjatywy podmiotów zobowiązanych – również w drodze przekazania zgłoszenia, w przypadku gdy dany podmiot zobowiązany wie, podejrzewa lub ma uzasadnione podstawy, by podejrzewać, że określone środki finansowe, niezależnie od kwoty, o jaką chodzi, są dochodami pochodzącymi z działalności przestępczej lub są powiązane z finansowaniem terroryzmu, a także na niezwłocznym odpowiadaniu na wnioski jednostki analityki finansowej o udzielenie dodatkowych informacji w takich przypadkach[12]. Wskazana jednostka analityki finansowej to centralna, państwowa agencja, która jest odpowiedzialna za otrzymywanie (oraz, jeśli to dozwolone, wnioskowanie), analizę i przekazywanie odpowiednim organom ujawnionych informacji finansowych, dotyczących podejrzanych dochodów i potencjalnego finansowania terroryzmu lub wymaganych przez krajowe prawodawstwo lub przepisy, w celu zwalczania prania pieniędzy

[10] https://eur-lex.europa.eu/legal-content/PL/LSU/?uri=celex:32015L0849.

[11] *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Wolters Kluwer, Warszawa 2020.

[12] Dyrektywa Parlamentu Europejskiego i Rady zmieniająca dyrektywę (UE) 2018/843 z 30.05.2018 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, Dz. Urz. UE nr L 156/43 (VDAML) doprecyzowała art. 33 ust. 1 lit. b) dyrektywy IVDAML, który otrzymał brzmienie „b) bezpośrednim dostarczaniu jednostce analityki finansowej, na jej wniosek, wszelkich niezbędnych informacji”.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

i finansowania terroryzmu[13]. Kolejną kwestią jest bezpośrednie dostarczanie tej jednostce na jej wniosek wszelkich niezbędnych informacji. Należy zwrócić uwagę, że takie informacje należy przekazać jednostce analityki finansowej państwa członkowskiego, na którego terytorium ma siedzibę podmiot zobowiązany, który przekazuje wskazane informacje[14].

Ostatecznie zgodnie z powyżej przedstawionymi zapisami polski prawodawca uregulował je w krajowym akcie prawnym, tj. ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Jak już wcześniej zasygnalizowano w art. 8 tejże ustawy zobowiązano instytucje obowiązane do wyznaczenia pracownika odpowiedzialnego za nadzór nad zgodnością działalności tej instytucji z ustawą. Przepis ten stanowi transpozycję art. 8 ust. 4 pkt a dyrektywy AML IV, który to z kolei nakazuje państwom członkowskim zapewnienie, aby instytucje obowiązane wyznaczyły pracownika odpowiedzialnego za zapewnienie zgodności z odpowiednimi przepisami i kontrolę pracowników. Co do zasady jednak pracownikiem tym nie musi być osoba, która współpracuje z daną instytucją obowiązaną na zasadzie umowy o pracę[15]. Osobę taką można nazwać AML Oficerem (AMLO). W zakres jego obowiązków oprócz wspomnianych powyżej powierza się także przekazywanie w imieniu instytucji obowiązanej zawiadomień, o których mowa w art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 1 i art. 90 u.p.p.p.f.t., a co za tym idzie osoba ta będzie nosiła miano *Money Laundering Reporting Officer* (MLRO), tj. pracownika do raportowania transakcji. Dlatego też interpretacja art. 8 u.p.p.p.f.t. nie powinna zmierzać do tego, że obowiązki AMLO oraz MLRO powinna wykonywać zawsze jedna i ta sama osoba. W praktyce większe podmioty ze względów organizacyjnych posiadają zarówno AMLO, który ponosi odpowiedzialność za *compliance* oraz kontrolę wewnętrzną, jak i MLRO, który zajmuje się analizą wszelkich wpływających sygnałów, a także oceną i raportowaniem transakcji, które trzeba zgłosić do jednostki analityki finansowej, tj. do Generalnego Inspektora Informacji Finansowej (GIIF). Gwoli ścisłości, art. 9 u.p.p.p.f.t precyzuje, że w przypadku przedsiębiorców prowadzących jednoosobową działalność gospodarczą funkcje AMLO, MLRO i osoby wykonującej czynności wskazane w ustawie pełni ta sama osoba. Natomiast należy wskazać, że treści artykułu nie powinno się interpretować w taki sposób, że łączenie tych funkcji jest możliwe tylko i wyłącznie w przypadku osób prowadzących jednoosobową działalność gospodarczą, ponieważ ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu nie zabrania łączenia rzeczonych funkcji w innych podmiotach[16]. Warto zaznaczyć, że MLRO odgrywa kluczową

[13] Art. 1 pkt f Konwencji Rady Europy z dnia 16 maja 2005 r. o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu (Dz.U. z 2008 r., nr 165, poz. 1028).

[14] Art. 33 ust. 1 lit. b zmieniona przez art. 1 pkt 21 dyrektywa nr 2018/843 z dnia 30 maja 2018 r. (Dz.U. UE. L. z 2018 r., nr 156, poz. 43) zmieniającego nin. dyrektywę z dniem 9 lipca 2018 r.

[15] *Przeciwdziałanie…*

[16] *Ibidem.*

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

rolę w tworzeniu przepisów dotyczących przeciwdziałania praniu pieniędzy. Jest odpowiedzialny za zgłaszanie wszelkich informacji i wątpliwości dotyczących przestępstw finansowych odpowiednim organom. MLRO to osoba, która podejmuje decyzje o raportowaniu, co może wpłynąć na relacje firmy z jej klientem oraz narazić na działania karne, prawne, regulacyjne i dyscyplinarne. Poza tym MLRO powinien wziąć na siebie odpowiedzialność za zapewnienie bezpieczeństwa wszystkich plików klienta i informacji biznesowych oraz że zostaną wykorzystane w celu podjęcia niezbędnych decyzji[17].

Funkcja AMLO stanowi integralną część ram zarządzania podmiotem, jakim jest instytucja obowiązana. Należy zwrócić uwagę, iż ustawodawca nakłada na instytucje obowiązane obowiązek przygotowania i przyjęcia wewnętrznych procedur kontroli (w tym także wewnętrznej procedury anonimowego zgłaszania rzeczywistych lub potencjalnych naruszeń) i zarządzania ryzykiem, przez co konieczne jest wyznaczenie określonych podmiotów, odgrywających określone role w całościowym systemie AML/CFT[18]. Co więcej, nowelizacja u.p.p.p.f.t. z dniem 31 lipca 2021 r. rozszerzyła katalog instytucji obowiązanych, dzięki czemu możliwe jest powołanie i funkcjonowanie AMLO w kolejnych podmiotach. Nie oznacza to jednak, że funkcjonowanie AML Oficera nie jest możliwe w innego rodzaju instytucjach, tj. takich, które nie spełniają wymogów określonych w art. 2 ust. 1 u.p.p.p.f.t. Natomiast w takim przypadku należy zwrócić uwagę, czy powołanie AMLO nie odbyło się jedynie dla pozoru lub wprowadzenia w błąd kontrahentów, gdyż w takiej sytuacji podmiot ten nie podlega reżimowi prawnemu określonemu w u.p.p.p.f.t., a co za tym idzie brak jest niezależnego podmiotu, którego zadaniem jest weryfikacja i nadzór nad realizowanym obowiązkiem zgodności w kwestiach AML/CFT. Z drugiej zaś strony podmiot, który nie zalicza się do instytucji obowiązanych, a mimo to powołuje Oficera AML, zwiększa swój status pewności na gruncie relacji z kontrahentem. Jednak, jak wskazuje art. 17 ust. 1 u.p.p.p.f.t., GIIF może zawierać porozumienia z podmiotami innymi niż instytucje obowiązane, a porozumienie to powinno zawierać zakres, formę i tryb przekazania informacji, który natomiast może przybrać formę raportowania AML/CFT. W takim przypadku na potrzeby współpracy z jednostką analityki finansowej będzie możliwe ustanowienie MLRO.

Szeroki zakres podmiotowy, który został zawarty w art. 2 ust. 1 u.p.p.p.f.t., kształtuje różnego rodzaju podmioty jako instytucje obowiązane według kryterium, jakim jest posiadany status formalnoprawny czy też ze względu na posiadane w swoich strukturach ograny[19]. Dlatego też należy odpowiednio wyznaczyć, m.in.

[17] https://sanctionscanner.com/knowledge-base/money-laundering-reporting-officer-mlro-125.

[18] https://assets.kpmg/content/dam/kpmg/pl/pdf/2021/05/pl-pl-alert-kpmg-2020-05-17-nowelizacja-ustawy-o-przeciwdzialaniu-praniu-pieniedzy-oraz-finansowaniu-terroryzmu.pdf.

[19] A. Golonka, *Zakres podmiotowy ustawy z przeciwdziałania praniu pieniędzy w świetle znowelizowanych przepisów*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2020, nr 82(3), s. 155–168.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

zgodnie z wewnętrznymi przepisami, uprawniony podmiot, który będzie odpowiedzialny za wykonanie określonego działania. W celu wyznaczenia odpowiednich pracowników należy posiłkować się art. 8 u.p.p.p.f.t. w konfiguracji z art. 6 i 7 tejże ustawy. Zaznaczyć należy, że AML Oficerem może zostać osoba, która dotychczas pracowała w instytucji obowiązanej lub zupełnie nowa osoba zatrudniona przez dany podmiot. Wyznaczenie może odbyć się w formie czynności formalno-prawnej lub pisma skierowanego do konkretnego pracownika albo w przypadku zatrudnienia nowej osoby poprzez zawarcie umowy o pracę z wyznaczeniem zakresu obowiązków AML/CFT. Interpretując art. 6, 7 i 8 u.p.p.p.f.t. należy zwrócić uwagę, że hierarchicznie są w nich wymienione osoby odpowiedzialne za wdrożenie systemu AML/CFT. Poczynając od art. 6, gdzie wymieniona została kadra kierownicza wyższego szczebla, przez którą rozumie się członka zarządu, dyrektora lub pracownika instytucji obowiązanej posiadającego wiedzę z zakresu ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z działalnością instytucji obowiązanej oraz podejmującego decyzje mające wpływ na to ryzyko. Natomiast w art. 7 wskazuje, że w przypadku instytucji obowiązanej, w której działa zarząd lub inny organ zarządzający, wyznacza się spośród członków tego organu osobę odpowiedzialną za wdrażanie obowiązków określonych w ustawie. Wyłoniony decydent spośród tych osób wyznaczy zaś zgodnie z art. 8 pracownika, który zajmuje kierownicze stanowisko i będzie odpowiedzialny za zapewnienie zgodności działalności instytucji obowiązanej z przepisami AML/CFT, a nadto za raportowanie transakcji do GIIF. AMLO rozpoczynając pracę powinien mieć jasno sformułowany zakres i sposób funkcjonowania, ale także określone obowiązki i uprawnienia. Wart uwagi jest fakt, że w przypadku gdy instytucja obowiązana przewiduje wprowadzenie odrębnych stanowisk dla AMLO, MLRO i AMLCO, to jednocześnie konieczne jest stworzenie wewnętrznych regulacji w zakresie relacji między nimi na obszarze nadzoru, podległości czy rozliczalności.

2.3. OBOWIĄZKI AMLO, MLRO

Jak już wcześniej zasygnalizowano do zadań AML Oficera zgodnie z art. 8 u.p.p.p.f.t. należy m.in. zapewnienie zgodności działalności instytucji obowiązanej oraz jej pracowników i innych osób wykonujących czynności na rzecz tej instytucji obowiązanej z przepisami o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Jest to najszerszy merytorycznie zakres działania AMLO, który wynika zarówno z samej ustawy, jak i z regulacji wewnętrznych z niej wynikających. AMLO w swoich działaniach powinien również kierować się przepisami wykonawczymi oraz polityką i ładem korporacyjnym, które z kolei odnoszą się do kwestii związanych z przeciwdziałaniem ML/FT. AML Oficer powinien elastycznie reagować na dynamiczne działania w instytucji obowiązanej. Nato-

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

miast zgodnie z art. 50 u.p.p.p.f.t. podstawowym dokumentem w instytucji obowiązanej, który powinien powstać z inicjatywy AMLO jest wewnętrzna procedura w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Procedura ta powinna być indywidualnie dostosowana do danego typu instytucji obowiązanej z uwzględnieniem charakteru jej działalności i rozmiaru. Musi być spójna z oceną ryzyka i działaniami w obszarze AML[20]. Zadaniem AMLO jest uczestniczenie w procesie tworzenia niniejszej procedury, merytoryczne jej redagowanie oraz finalnie przedstawienie jej kadrze kierowniczej wyższego szczebla do akceptacji. Wewnętrzna procedura AML jest o tyle istotna, że jest dokumentem stanowiącym swoistą podstawę działalności AML Oficera w zakresie wykonywania zadań zgodnościowych, jak również monitorowania realizacji, a także oceny, czy ta zgodność jest realizowana. Należy również wziąć pod uwagę, że jeżeli według tego dokumentu ma działać AMLO to także na jego podstawie może być oceniany przez kadrę kierowniczą wyższego szczebla, gdyż pozwoli to ocenić prawidłowość i efektywność jego działań. Takie działania są skuteczne w zapobieganiu odpowiedzialności administracyjnej, a przez to nałożeniu wysokich kar, które może nałożyć organ kontroli zarówno na samego AMLO, jak i kadrę kierowniczą wyższego szczebla. Dodatkowo instytucje obowiązane powinny stosować wobec swoich klientów odpowiednie środki bezpieczeństwa finansowego. Zakres i intensywność danych środków bezpieczeństwa zależą jednak od rozpoznanego ryzyka narażenia na udział w procederze prania pieniędzy lub finansowania terroryzmu. Do ustawowych środków bezpieczeństwa finansowego należy zaliczyć:

- identyfikację klienta oraz weryfikację jego tożsamości,
- identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości, oraz ustalenia struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej,
- ocenę stosunków gospodarczych klienta oraz (stosownie do sytuacji) uzyskanie informacji na temat ich celu i zamierzonego charakteru,
- bieżące monitorowanie stosunków gospodarczych klienta, w tym:
  - analiza transakcji przeprowadzanych w ramach stosunków gospodarczych w celu zapewnienia, że transakcje te są zgodne z wiedzą instytucji obowiązanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz zgodne z ryzykiem prania pieniędzy oraz finansowania terroryzmu związanym z tym klientem,
  - badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta w przypadkach uzasadnionych okolicznościami,
  - zapewnienie, że posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych są na bieżąco aktualizowane[21].

[20] https://rpms.pl/dokumenty-aml/.

[21] https://www.iaml.com.pl/wiedza/obowiazki-instytucji-obowiazanych/.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Kolejnym zadaniem AMLO jest przekazywanie w imieniu instytucji obowiązanej zawiadomień, o których mowa w art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 1 i art. 90 u.p.p.p.f.t. Ściślej mówiąc MLRO zobowiązany jest do zawiadamiania GIIF o wszelkich okolicznościach budzących wątpliwości, a co za tym idzie, okolicznościach, które mogą wskazywać, że zachodzi podejrzenie popełnienia przestępstwa w zakresie prania pieniędzy lub finansowania terroryzmu. Są to zawiadomienia opisowe, tzw. SARy (*Suspicious Activity Reports*), które są przekazywane do organu kontroli zazwyczaj w trybie przewidzianym w u.p.p.p.f.t. w:

- art. 74 (zawiadomienie od instytucji obowiązanej o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu), oraz
- art. 86 (zawiadomienie od instytucji obowiązanej o przypadku powzięcia uzasadnionego podejrzenia, że określona transakcja lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu)[22].

W przygotowaniu zawiadomienia można posiłkować się wskazówkami zawartymi w 22 Komunikacie GIIF w sprawie praktycznych aspektów stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień. Wynika z niego, że zawiadomienie złożone w trybie art. 74 jest stosowane w sytuacji, gdy instytucja obowiązana już zidentyfikowała podejrzane okoliczności, które mogą wskazywać na pranie pieniędzy, a nadto ma wątpliwości w zakresie stosowania środków bezpieczeństwa finansowego. Zawiadomienie to musi być szczegółowo opisane i uzasadnione, po czym przekazane do Generalnego Inspektora niezwłocznie, nie później jednak niż w terminie 2 dni roboczych od dnia potwierdzenia przez instytucję obowiązaną tego podejrzenia. Natomiast zawiadomienie z art. 86 stosowane jest w przypadku, kiedy instytucja obowiązana powzięła jedynie uzasadnione podejrzenie prania pieniędzy, a mianowicie posiada dowody lub przypuszczenia, które wskazują na pranie pieniędzy lub finansowanie terroryzmu. Należy zwrócić uwagę, że głównym celem tego zawiadomienia jest zablokowanie środków i poinformowanie GIIF o zaistniałej sytuacji, a co za tym idzie podjęcie z nim ścisłej współpracy, a na późniejszym etapie podjęcie współpracy również z właściwymi organami ścigania[23]. Generalny Inspektor natomiast przeka-

[22] W. Gibas, *Zawiadomienie do Generalnego Inspektora Informacji Finansowej*, https://pl.linkedin.com/pulse/zawiadomienie-do-generalnego-inspektora-informacji-finansowej-gibas (data dostępu: 24 sierpnia 2021).

[23] Komunikat nr 22 w sprawie praktycznych aspektów stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień, o których mowa w art. 74 i art. 86 ustawy AML, https://www.gov.pl/web/finanse/komunikat-nr-22-w-sprawie-praktycznych-aspektow-stosowania-srodkow-bezpieczenstwa-finansowego-oraz-przekazywania-zawiadomien-o-ktorych-mowa-w-art-74-i-art-86-ustawy-aml2.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

zuje osobie zgłaszającej informacje na temat działań, jakie mogą być podejmowane po przyjęciu zgłoszenia[24].

Do obowiązków MLRO należy zaliczyć:

- podjęcie decyzji, czy wymagane jest wystarczające podejrzenie do generowania raportów na temat prania pieniędzy, a także odpowiednie ujawnienie ich odpowiednim władzom.
- obserwowanie i planowanie nowych przepisów, które dotyczą opracowywania polityk, systemów i procedur przeciwdziałania praniu pieniędzy w celu zapewnienia skutecznego ich wdrażania.
- dbanie o to, kogo wdraża jako klienta. W ramach programu AML zgodność z KYC (*Know-Your-Customer/Client*) odgrywa tutaj swoją rolę, a sam proces KYC rozpoczyna się przed nawiązaniem jakiejkolwiek relacji biznesowej i trwa przez całą relację.
- umiejętność oceny ryzyka przestępstw finansowych, identyfikowanie problemów w procesach *compliance* i ich analiza.
- ostatnim, ale nie mniej ważnym zakresem działań AMLO są powierzone do wykonania inne zadania związane z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu. Do takich zadań można zaliczyć m.in.:
- nadzorowanie i weryfikację oceny ML/FT opartej o ryzyko,
- przygotowanie wewnętrznego regulaminu, w myśl art. 50 u.p.p.p.f.t.,
- organizowanie szkoleń zewnętrznych dla wyznaczonych pracowników,
- samokształcenie, tj. udział z kursach, szkoleniach, sympozjach, spotkaniach o tematyce *AML*/CFT,
- współpraca z prokuraturą i służbami będącymi jednostkami współpracującymi (Policja, ABW, CBA, KAS)[25].

Niekiedy wydawać się może, że pewne czynności należą jedynie do obowiązków osób wskazanych w art. 6 i 7 u.p.p.p.f.t., gdyż AMLO nie ma umocowania do ich wykonania, jednak może on w tym zakresie przygotowywać wszelkie dokumenty, analizy czy oceny i realizować polecenia kadry kierowniczej wyższego szczebla. Wyjątek stanowi instytucja z art. 9 ustawy, ponieważ w tym przypadku możliwe jest wykonanie wszelkich obowiązków nałożonych na instytucję obowiązaną przez jedną osobę. Dodatkowo, jeśli zakres obowiązków AMLO tak stanowi, możliwa jest współpraca zewnętrzna z jednostkami współpracującymi[26].

[24] Rozporządzenie Ministra Finansów z dnia 16 maja 2018 r. w sprawie odbierania zgłoszeń o naruszeniu przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., 959).

[25] M.A. Kędzierski, *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, http://www.abw.gov.pl/download/1/2984/MKedzierski-POL.pdf.

[26] Jednostki współpracujące – pod tym pojęciem rozumie się organy administracji rządowej, organy jednostek samorządu terytorialnego oraz inne państwowe jednostki organizacyjne, a także

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Warto zauważyć, że instytucje obowiązane zazwyczaj stawiają na równi obowiązki i zakres działania OC oraz AMLO. Jednak jest to mylne założenie z uwagi na fakt, że kompetencje *compliance* oficera wykraczają poza obszar AML i wchodzą w zakres obowiązków mających na celu kompleksowe zapewnienie danemu podmiotowi reguł i procedur zgodnościowych. Natomiast obowiązki AMLO określone są w u.p.p.p.f.t., które z kolei można podzielić na różne kategorie, tj. raportowanie do jednostki analityki finansowej (MRLO), działanie zgodnościowe w obszarze AML/CFT (AMLCO), ale także inne zadania, m.in. związane z predykcją produktów i usług, które mają zostać wprowadzone na rynek pod kątem ich ryzyka bezpieczeństwa w danym obszarze. Niemniej podmioty te powinny współpracować ze sobą i wzajemnie się wspierać w odniesieniu do oceny ryzyka bezpieczeństwa instytucji. Na marginesie należy wspomnieć, iż w przypadku funkcjonowania tych dwóch podmiotów na poziomach nadrzędności to rolę nadrzędną będzie pełnił CO, co będzie miało znaczenie w przypadku powierzenia i wykonywania określonych obowiązków. W takim przypadku nie bez znaczenia pozostaje wielkość, struktura i zakres działania instytucji obowiązanej.

Godny uwagi jest fakt, że ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw[27] wprowadziła ochronę prawną pracownika w art. 53 ust. 2 pkt 3 i 4, a w tym AMLO, poprzez zapewnienie ochrony pracownika lub innej osoby wykonującej czynności na rzecz instytucji obowiązanej dokonujących zgłoszenia, zapewniając co najmniej ochronę przed działaniami o charakterze represyjnym lub wpływającymi na pogorszenie ich sytuacji prawnej lub faktycznej, lub polegającymi na kierowaniu gróźb. Co więcej instytucja obowiązana i jej pracownicy są zobowiązani do ochrony danych osobowych tych osób oraz osoby, której zarzuca się dokonanie naruszenia, zgodnie z przepisami o ochronie danych osobowych. Wszelkie naruszenia w tej kwestii mogą być zgłoszone przez osoby narażone na represje do GIIF. Dotyczy to zarówno represji ze strony podmiotów zewnętrznych, jak i wewnętrznych, tj. pracowników struktury instytucji obowiązanej.

2.4. ODPOWIEDZIALNOŚĆ AMLO, MLRO

Definicja przestępstwa prania pieniędzy, a w związku z tym także sankcje za jego popełnianie zostały określone po raz pierwszy na gruncie polskiego prawa w ustawie z dnia 12 października 1994 r. o ochronie obrotu gospodarczego

Narodowy Bank Polski, Komisję Nadzoru Finansowego i Najwyższą Izbę Kontroli (art. 2, ust. 2, pkt 8 u.p.p.p.f.t).

[27] Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r., poz. 815).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

i zmianie niektórych przepisów prawa karnego[28]. Zidentyfikowano w niej wąski katalog możliwych przestępstw bazowych[29], związanych z przestępczością zorganizowaną. Podobnie postąpiono opisując pranie pieniędzy w pierwszym brzmieniu art. 299 kk[30].

Obecnie, jak wynika z art. 58 ust. 3 dyrektywy AML IV, który jest implementowany do prawa krajowego przez art. 154 ust. 1 u.p.p.p.f.t., państwa członkowskie zostały zobligowane do wprowadzenia możliwości stosowania kar i środków wobec członków organu zarządzającego instytucji obowiązanych i innych osób fizycznych odpowiedzialnych za naruszenia przez instytucje obowiązane przepisów AML/CFT. Jak wskazano powyżej, CO różni się od AMLO, w związku z czym różna jest też ich odpowiedzialność, ze względu na to, iż AMLO podlega u.p.p.p.f.t., natomiast CO już nie. Przy czym pod rozwagę należy wziąć zakres odpowiedzialności tych osób, ponieważ co do zasady CO będzie ponosił odpowiedzialność za zorganizowanie systemu zarządzania zgodnością, natomiast nie za poszczególne naruszenia. Niektóre instytucje obowiązane, jak np. banki tworzą swego rodzaju wzorce zgodnościowe m.in. w zakresie AML/CFT. Przykładem mogą być Rekomendacje H przygotowane przez Komisję Nadzoru Finansowego, które dotyczą wewnętrznej kontroli[31]. Jeśli zatem dana instytucja posiada tego typu regulacje, czynności zgodnościowe dokonywane przez instytucję należy dostosować do specyfiki jej działalności. Natomiast zakres obowiązków AMLO i CO dotyczący realizacji rekomendacji powinien być zawarty w wewnętrznych systemach organizacyjnych instytucji. Warto zaznaczyć, że zawód, jakim jest CO, nie został uregulowany w żadnej dziedzinie prawa, dlatego zakres jego obowiązków będzie uregulowany jedynie w umowie, a jego odpowiedzialność może być regulowana w sposób dowolny. Dodatkowo jego zadania są zależne od przeprowadzenia analizy ryzyka wystąpienia nieprawidłowości, które co do zasady różnią się w zależności od przedsiębiorstwa[32]. Wracając jednak do różnic między CO a AMLO, mimo iż odpowiadają oni w różnym zakresie, to jednak za ten sam odcinek, jakim jest zgodność instytucji obowiązanej z przepisami, regulaminami, zasadami na poziomie krajowym, jak i międzynarodowym. Źródeł zakresu odpowiedzialności AMLO

[28] Dz.U. nr 126, poz. 615.

[29] Pojęcie przestępstwa bazowego odnosi się do czynów karalnych, z których mogą pochodzić korzyści majątkowe podlegające praniu. Zostało ono także zdefiniowane w art. 1 lit. e Konwencji Rady Europy z dnia 16 maja 2005 r. o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu jako każde przestępstwo, wskutek którego zostały uzyskane dochody mogące być przedmiotem przestępstwa prania pieniędzy.

[30] *Krajowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu*, Ministerstwo Finansów, Warszawa 2019.

[31] Komisja Nadzoru Finansowego, Rekomendacje H dotycząca systemu kontroli wewnętrznej w bankach, Warszawa, kwiecień 2017, https://www.knf.gov.pl/knf/pl/komponenty/img/knf_170534_Rekomendacja_H_2017_50303.pdf.

[32] M. Małolepszy, M. Pierzchlewicz, *Odpowiedzialność karna oficera compliance*, „Prokuratura i Prawo" 2019, nr 5, s. 8.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

szukać należy również w umowie, tak jak w przypadku CO, ale przede wszystkim w ustawach, a w szczególności u.p.p.p.f.t., która precyzuje zakres obowiązków, ale również odpowiedzialność administracyjną i karną za ich naruszenie. Dodatkowo art. 154 ust. 1 u.p.p.p.f.t. wskazuje, że na AMLO spoczywa także odpowiedzialność finansowa. Kara ta może zostać nałożona zarówno na członka zarządu, jak i na kadrę kierowniczą wyższego szczebla czy pracownika zajmującego kierownicze stanowisko odpowiedzialnego za zapewnienie zgodności działalności instytucji obowiązanej oraz jej pracowników z przepisami AML (MRLO)[33]. Należy zaznaczyć, że jeśli w instytucji obowiązanej odrębnie funkcjonują AMLCO i MRLO, to każda odpowiada zgodnie z zakresem swoich obowiązków. Dlatego też tak ważne jest właściwe wyznaczenie odpowiedniego pracownika na konkretne stanowisko ze szczegółowym wskazaniem zakresu jego obowiązków.

Jak już wcześniej zasygnalizowano, AMLO zgodnie z u.p.p.p.f.t. może ponieść odpowiedzialność karną lub administracyjną (delikt administracyjny). Odpowiedzialność karną reguluje u.p.p.p.f.t. oraz kodeks karny[34]. W art. 2 ust. 2 pkt 14 u.p.p.p.f.t. przewidziane jest odesłanie do art. 299 k.k. spełniające postulat VI dyrektywy AML[35] w zakresie opisu typu czynu zabronionego, który zaś odnosi się do konieczności ujednolicenia definicji wskazanego przestępstwa w systemach prawnych państw członkowskich UE. Kwestia charakterystyki zachowania przestępnego zarówno w ustawodawstwie polskim, jak i w art. 3 ust. 1 VIDAML jest zgodna w zakresie znamion strony podmiotowej (umyślności), jak i przedmiotowej (opisu czynności wykonawczej). Warto podkreślić, że prawodawca unijny przesłanką karalności czyni jedynie zachowanie sprawcy, które zostało powzięte w warunkach świadomości co do jego nielegalnego pochodzenia, a to w polskim systemie prawa karnego pozostaje immanentną cechą umyślności[36]. Postanowienia zawarte w art. 3 VIDAML wprowadzają również możliwość objęcia penalizacją także nieumyślności. W świetle polskich przepisów karnych (art. 9 § 2 k.k.) czyn zabroniony popełniony jest nieumyślnie wtedy, gdy sprawca nie ma zamiaru jego popełnienia, ale wskutek niezachowania ostrożności wymaganej w danych okolicznościach popełnia taki czyn, mimo iż możliwość popełnienia tego czynu przewidywał albo mógł przewidzieć[37]. Z kolei art. 2 ust. 2 pkt 6 u.p.p.p.f.t. odsyła do

[33] M. Ajs, A. Widzewicz, *Rozszerzenie odpowiedzialności za naruszenie obowiązków dotyczących przeciwdziałania praniu pieniędzy*, https://www.prawo.pl/ biznes/wieksza–odpowiedzialnosc–i–wyzsze–kary–za–naruszenie–obowiazkow,496338.html.

[34] Ustawa z dnia 6 czerwca 1997 r., Kodeks karnyz dnia 25 sierpnia 2020 r.,, t.j. Dz.U. z 2020 r., 1444 zwana dalej k.k.

[35] Dyrektywa Parlamentu Europejskiego I Rady (UE) 2018/1673 z dnia 23 października 2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych, online: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018L1673&from=HU.

[36] Art. 9, *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, Wolters Kluwer, Warszawa 2021.

[37] A. Golonka, *Polskie regulacje karne wobec „szóstej ”dyrektywy Anti-Money Laundering”*, „Iusnovum” 2021, nr 1.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

art. 165a k.k., co wskazuje, iż zarówno pranie pieniędzy, jak i finansowanie terroryzmu są przestępstwami, a nie jedynie deliktami administracyjnoprawnymi. Z drugiej jednak strony do realizacji przez państwa członkowskie UE obowiązku przeciwdziałania tym przestępstwom niezbędne są działania zapobiegające wykorzystywaniu systemu finansowego rozumianego zarówno jako system obrotu gotówkowego, jak i bezgotówkowego. Zgodnie bowiem z motywem 5 preambuły IVDAML „wykorzystywanie systemu finansowego do kierowania pieniędzy pochodzących z nielegalnego, a nawet z legalnego źródła na cele terrorystyczne stwarza wyraźne ryzyko dla integralności, prawidłowego funkcjonowania, wiarygodności i stabilności systemu finansowego”[38].

Natomiast jeśli chodzi o u.p.p.p.f.t., to odpowiedzialność karna została uregulowana w rozdziale 14 w zaledwie dwóch artykułach. Pierwszym z nich jest art. 156, który w ust. 1 wskazuje, że kto, działając w imieniu lub na rzecz instytucji obowiązanej nie dopełnia obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, lub obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o powzięciu uzasadnionego podejrzenia, że określona transakcja lub wartości majątkowe będące przedmiotem tej transakcji mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, przekazuje Generalnemu Inspektorowi nieprawdziwe lub zataja prawdziwe dane dotyczące transakcji, rachunków lub osób, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Ustęp 2 zaś uznaje, że tej samej karze podlega, kto wbrew przepisom ustawy ujawnia osobom nieuprawnionym, posiadaczom rachunku lub osobom, których transakcja dotyczy, informacje zgromadzone zgodnie z ustawą lub wykorzystuje te informacje w sposób niezgodny z przepisami ustawy. Wydawać by się mogło, że opisane powyżej przestępstwa można popełnić jedynie umyślnie, ale ustawa przewiduje, iż sprawca czynu określonego w ust. 1 pkt 1 lub ust. 2 działając nieumyślnie podlega grzywnie. Tak więc można wnioskować, że celem ustawodawcy jest pociągnięcie do odpowiedzialności osób, które są zobowiązane do wykonywania obowiązków wynikających z ustawy (art. 7 i 8). Niedopełnienie obowiązków ustawowych wskazane w art. 156 ust. 1 pkt 1 odnosi się do zawiadomień o podejrzeniu prania pieniędzy lub finansowania terroryzmu (art. 74 ust. 1 u.p.p.p.f.t.) oraz o uzasadnionym podejrzeniu, że określona transakcja lub określone wartości majątkowe są związane z praniem pieniędzy lub finansowaniem terroryzmu (art. 86 ust. 1 u.p.p.p.f.t.)[39]. Jeśli chodzi naruszenie przez AMLO art. 156 ust. 1 pkt 2 u.p.p.p.f.t., to naruszenie takie może nastąpić jedynie na skutek świadomego działania lub rażącego zaniedbania. Dla przykładu w sytuacji, gdy AMLO przekaże GIIF niezgodne dane ze stanem rzeczywistym

[38] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie, VI SA/Wa 2690/20, brak podstaw do odstąpienia od wszczęcia postępowania, LEX, nr 3209323.

[39] *Przeciwdziałanie*...

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

spowoduje to fałszywy obraz stanu faktycznego co będzie działaniem. Z kolei zatajenie prawdziwych danych może być traktowane jako działanie, ale także jako zaniechanie. Warto zauważyć, że identyfikacja, weryfikacja i monitoring klienta, który jest realizowany w zakresie stosowania środków bezpieczeństwa finansowego, powinien w swoim zakresie obejmować również ustalenie i ocenę prawdziwości danych. Wynika z tego, że AMLO nie poniesie odpowiedzialności za przekazanie nieprawdziwych danych w przypadku, gdy nie będzie miał możliwości ich weryfikacji przed przekazaniem do GIIF. Natomiast w takim przypadku może ponieść odpowiedzialność za nieodpowiednie przygotowanie, zgodnie z art. 50 ust. 1 u.p.p.p.f.t., procedury wewnętrznej, ale także za niesprawność całego systemu zgodności, a co za tym idzie poniesienie odpowiedzialności karnej z art. 156 ust. 1 pkt 2 u.p.p.p.f.t. W kwestii odpowiedzialności istotny jest podział obowiązków w instytucji obowiązanej oraz zakres podejmowanych decyzji, ponieważ jeśli w instytucji obowiązanej występuje AMLO i MRLO, to właśnie za raportowanie lub naruszenie tego obowiązku będzie odpowiadał MLRO. Innymi słowy będzie on odpowiadał w sytuacji, gdy wykrył podejrzane transakcje w toku działań instytucji obowiązanej, a mimo to nie przekazał ich do GIIF i tym samym nie nadał sprawie dalszego biegu. W związku z czym GIIF nie zawiadomił właściwego prokuratora, który we współpracy z organami ścigania miałby podjąć działania w celu postawienia aktu oskarżenia podejrzanym osobom za przestępstwa z art. 299 k.k. lub art. 165a k.k.[40]. Jak powszechnie wiadomo pranie pieniędzy to proceder wielofazowy obejmujący różne następujące po sobie czynności. Ich celem jest asymilacja środków pochodzących z przestępstwa przez kapitał pochodzący z legalnych źródeł. Czynności te mogą polegać między innymi na ulokowaniu ich na pierwszym, pierwotnym koncie, by następnie poprzez mnożenie operacji finansowych, wykonanie jak największej liczby transakcji ukryć związek między współsprawcami przestępstwa w celu uniemożliwienia wykrycia źródła pochodzenia środków. Następnie dochodzi do włączenia tychże pieniędzy do kapitału pochodzącego z legalnych źródeł. Dla realizacji znamion z art. 299 k.k. nie jest konieczne działanie mające na celu wprowadzenie brudnych pieniędzy do obrotu. Odpowiedzialności prawnej podlega bowiem sprawca, który ukrywa pieniądze lub je przyjmuje także w innym celu np. w celu osiągnięcia korzyści majątkowej[41].

Jak wskazuje T. Mierzwiński, sprawcą przestępstwa może być tylko i wyłącznie osoba fizyczna działająca w imieniu i na rzecz instytucji obowiązanej, bez względu na formę zatrudnienia, i podlega karze pozbawienia wolności od 3 miesięcy do lat 5[42]. Natomiast przy ustaleniu znamion przestępstwa określonego w art. 156 u.p.p.p.f.t. należy wziąć pod uwagę, czy MLRO przygotował i wprowadził w życie

[40] https://www.gov.pl/web/finanse/przeciwdzialanie-praniu-pieniedzy-i-finansowaniu-terroryzmu.

[41] Wyrok Sądu Apelacyjnego w Warszawie II AKa 156/17, Analiza znamion prania pieniędzy, LEX, nr 2317774

[42] *Przeciwdziałanie…*

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

przepisy wykonawcze określone w art. 79 ust. 3 u.p.p.p.f.t. dotyczące rozporządzenia ministra właściwego do spraw finansów publicznych w zakresie sposobu sporządzania i przekazywania zawiadomienia, o którym mowa w art. 74, oraz informacji i dokumentów, o których mowa w art. 76, jak również tryb ich przekazywania, mając na uwadze konieczność sprawnego, wiarygodnego i bezpiecznego ich przekazywania. Na marginesie należy zaznaczyć, iż ani ustawa, ani rozporządzenia nie nakładają na MLRO żadnych obwarowań w zakresie nazewnictwa plików przesyłanych do GIIF. Instytucja obowiązana może zatem stosować dowolne nazewnictwo w tym zakresie, jednak zalecane jest stosowanie adekwatnej do własnych potrzeb metody nazewnictwa plików w celu zachowania porządku ich przechowywania[43]. Tak więc jeśli chodzi o penalizację inkryminowanego czynu z art. 156 ust. 1 pkt 2 u.p.p.p.f.t., to odpowiedzialność ponosi sprawca, który aktywnie przekazuje nieprawdziwe dane jednostce analityki finansowej lub też świadomie zataja prawdziwe dane, które powinien przedłożyć Generalnemu Inspektorowi. Dane „dotyczące transakcji, rachunków lub osób", które są przedmiotem przekazania do GIIF, mogą być łączone z dokonaną transakcją, ale nie jest to warunek konieczny, ponieważ mogą być to także dane związane z innym działaniem wewnątrzinstytucjonalnym w zakresie AML/CFT. Penalizacja dotyczy również takich sytuacji, kiedy to MLRO przekazuje nieprawdziwe dane z własnej inicjatywy, tylko po to, aby wprowadzić Generalnego Inspektora w błąd. Należy zwrócić jednak uwagę, że dotyczy to danych określonych w u.p.p.p.f.t. i przepisach wykonawczych, a zatem dotyczy to dokumentów pozostających w relacji między instytucją obowiązaną a GIIF[44]. Warto też zaznaczyć, że aby wypełnić znamiona przestępstwa, nie jest konieczne wywołanie błędu GIIF, który ma wpływ na jego postępowanie, ale również nieważny jest sposób przekazania danych Generalnemu Inspektorowi, tj. czy informacje te zostały doręczone wprost do niego, czy też elektronicznie do Departamentu Informacji Finansowej. W celu ustalenia sprawcy niezmiernie ważne jest ustalenie zakresu czynności AMLO, ponieważ od tego zależy jego odpowiedzialność. Jak już wcześniej wspomniano, jeżeli w instytucji obowiązanej obok AMLO występuje także MLRO, w którego zakres obowiązków wchodzi współdziałanie z GIIF oraz dostęp do weryfikacji i monitoringu danych, to będzie on uznany za sprawcę przestępstwa z art. 156 u.p.p.p.f.t. Z założenia MLRO posiada największą wiedzę z zakresu okoliczności i transakcji przekazywanych do GIIF. Co więcej, aby przekazać nieprawdziwe dane lub zataić prawdziwe, MLRO musi doskonale orientować się w obu przypadkach, jakie są prawdziwe dane dotyczące transakcji, rachunków i osób. Dodatkowo art. 77 u.p.p.p.f.t. ogra-

[43] Komunikat nr 8 w sprawie nadawania nazw plikom przekazywanym przez instytucje obowiązane do GIIF, zawierającym informacje o transakcjach ponadprogowych, o których mowa w art. 72 ustawy AML.

[44] M.A. Kędzierski, *Obowiązki i odpowiedzialność oficera AML (AMLO) w instytucji obowiązanej, cz. 2,* „Prokuratura i Prawo" 2021, nr 6, s. 45–72.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nicza udział innego pracownika instytucji obowiązanej w przekazywaniu informacji Generalnemu Inspektorowi. W sytuacji, gdy podczas kontroli ujawnione zostaną okoliczności, które wskazują na uzasadnione podejrzenie przestępstwa lub wykroczenia z art. 156 i art. 157 u.p.p.p.f.t., obowiązkiem osoby kontrolującej jest niezwłoczne zawiadomienie bezpośredniego przełożonego o zaistniałej sytuacji. W kolejnym koku Dyrektor Departamentu Informacji Finansowej Ministerstwa Finansów podejmuje decyzję w przedmiocie przekazania zawiadomienia o podejrzeniu popełnienia przestępstwa lub wykroczenia właściwemu organowi ścigania[45].

Drugim typem odpowiedzialności, jaką ponosi AMLO, jest odpowiedzialność za delikt administracyjny. Jak wskazuje art. 17 ust. 1 rozporządzenia 2015/847 „przewidziane kary i środki muszą być skuteczne, proporcjonalne i odstraszające, a ponadto spójne z karami określonymi zgodnie z rozdziałem VI sekcja 4 dyrektywy (UE) 2015/849"[46]. W związku z powyższym polski ustawodawca wprowadził w art. 148 u.p.p.p.f.t. regulacje w zakresie nałożenia kar administracyjnych za niedopełnienie obowiązków wynikających z przepisów unijnych. Naruszenie przez instytucje obowiązaną obowiązków określonych w art. 147 lub art. 148 u.p.p.p.f.t. powoduję nałożenie kar przez organy określone w art. 151 ust. 1 na osoby wskazane w art. 6–8 tejże ustawy. Innymi słowy kary i sankcje mogą być nałożone na instytucje obowiązane, w tym:

- na członków zarządu w spółkach, którzy zostali wskazani jako osoby odpowiedzialne za wykonanie obowiązków ustawowych,
- na kadrę kierowniczą wyższego szczebla lub pracownika zajmującego kierownicze stanowisko, który jest odpowiedzialny za zapewnienie zgodności działalności instytucji obowiązanej oraz jej pracowników z przepisami AML (MLRO),
- na mikroprzedsiębiorcę, który prowadzi jednoosobową działalność i nie wykonuje obowiązków wynikających z ustawy AML[47].

Jak wyżej wspomniano, karę może nałożyć Generalny Inspektor Informacji Finansowej, który sprawuje generalną kontrolę wykonywania przez instytucje obowiązane obowiązków AML/CFT, prezes NBP w odniesieniu do podmiotów prowadzących działalność kantorową w rozumieniu ustawy z dnia 27 lipca 2002 r. – Prawo dewizowe[48] oraz Komisja Nadzoru Finansowego w odniesieniu do instytucji obowiązanych przez nią nadzorowanych.

Należy wskazać, że karami administracyjnymi w myśl art. 150 ust. 1 u.p.p.p.f.t. są:

[45] *Ibidem*.

[46] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006.

[47] https://www.iaml.com.pl/wiedza/kary-sankcje-przeciwdzialanie-praniu-pieniedzy/.

[48] Ustawa z dnia 27 lipca 2002 r. Prawo dewizowe (Dz.U. z 2002 r., nr 141, poz. 1178).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- publikacja informacji o instytucji obowiązanej oraz zakresie naruszenia przepisów ustawy przez tę instytucję w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych;
- nakaz zaprzestania podejmowania przez instytucję obowiązaną określonych czynności;
- cofnięcie koncesji lub zezwolenia albo wykreślenie z rejestru działalności regulowanej;
- zakaz pełnienia obowiązków na stanowisku kierowniczym przez osobę odpowiedzialną za naruszenie przez instytucję obowiązaną przepisów ustawy, przez okres nie dłuższy niż rok;
- kara pieniężna.

Zastosowanie najlżejszej z kar, którą jest publikacja informacji o naruszeniu przepisów, może negatywnie wpłynąć na wiarygodność danej firmy, a w efekcie na jej problemy finansowe. Bardziej dolegliwe sankcje, np. cofnięcie koncesji, od razu eliminuje dany podmiot z rynku, natomiast wysoka kara pieniężna może bardzo szybko wykluczyć instytucję obowiązaną z możliwości dalszego funkcjonowania[49]. Zaznaczyć należy, iż wysokość kar finansowych zależy od kilku czynników, a mianowicie od tego, czy możliwe jest ustalenie korzyści kwoty korzyści lub straty wygenerowanej przez instytucję obowiązaną w związku z naruszeniem ustawy AML. Tym samym, jeśli jest to możliwe, to karę nakłada się do wysokości dwukrotności kwoty tej osiągniętej korzyści lub unikniętej straty, w przeciwnym wypadku równowartość kary może wynosić nawet do 1 000 000 euro. Kolejnym kryterium nałożenia kary są sytuacje szczególne, które kwalifikują podmiot do nałożenia na niego kary znacząco wyższej. Taka sytuacja może dotyczyć banków, spółdzielczych kas oszczędnościowo-kredytowych, firm inwestycyjnych, instytucji płatniczych i pożyczkowych, funduszy inwestycyjnych, firm i pośredników ubezpieczeniowych, a także przedsiębiorców prowadzących działalność np. kantorową czy polegającą na udostępnianiu skrytek sejfowych. W tym przypadku jednak wysokość kary różni się ze względu na sprawcę naruszenia, gdyż osoba fizyczna może otrzymać karę w wysokości do 20 868 500 zł, natomiast osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej nawet do 5 000 000 euro albo do wysokości 10% obrotu wykazanego w ostatnim zatwierdzonym sprawozdaniu finansowym za rok obrotowy lub w ostatnim skonsolidowanym sprawozdaniu finansowym za rok obrotowy. Ostatnią kwestia jest stwierdzenie naruszenia przez AMLO/MRLO określonych obowiązków (np. brak sporządzenia i aktualizacji oceny ryzyka, nieprzekazanie GIIF żądanych infor-

[49] P. Kaczmarek, *Kary w AML – co nam grozi?*, https://home.kpmg/pl/pl/blogs/home/posts/2021/05/blog-podatkowy-nowelizacja-ustawy-o-aml-uchwalona-30-marca-2021-roku-i-jej-wplyw-na-instytucje-obowiazane.html.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

macji, niewłaściwe stosowanie środków bezpieczeństwa finansowego, brak dokumentacji lub procedury wewnętrznej) oraz naruszenia obowiązków wynikających z rozporządzenia w sprawie informacji towarzyszących transferom środków pieniężnych, organy nadzorcze mogą nałożyć odrębną karę finansową na osobę odpowiedzialną za AML. W takiej sytuacji AMLO może zostać ukarany karą w wysokości do 1 000 000 zł[50].

Warto zwrócić jednak uwagę na fakt, że w zakresie odpowiedzialności za naruszenia z art. 147 i 148 u.p.p.p.f.t. ustawodawca odniósł się do podmiotów określonych w art. 6, 7 i 8 u.p.p.p.f.t. bez uwzględnienia różnic zadań i obowiązków poszczególnych osób. W związku z tym możliwe jest wyróżnienie określonych naruszeń i przypisanie ich do poszczególnych osób, chyba że wewnętrzne regulacje przewidują wspólną odpowiedzialność za naruszenia z art. 147 i 148 u.p.p.p.f.t. W instytucji obowiązanej może występować współodpowiedzialność, w sytuacji, gdy oprócz AMLO, który pełni funkcje nadzorujące i zarządzające, powołany jest podległy mu AMLCO i MRLO. Jeśli chodzi o art. 147 pkt 1 u.p.p.p.f.t., to odnosi się on nie tyle do AMLO, co do decydenta o jego wyznaczeniu, tj. osoby podlegającej zapisom art. 6 i 7 tejże ustawy. W zakresie kolejnego punktu (art. 147 pkt 2 i 3) odpowiedzialność ponosi już AMLO, który w swoim zakresie zadań ma obowiązek sporządzenia oceny ryzyka i przekazanie jej na żądanie GIIF. Jednak za tę kwestię odpowiedzialność może ponosić również przedstawiciel kadry kierowniczej wyższego szczebla posiadający wiedzę z zakresu ryzyka prania pieniędzy oraz finansowania terroryzmu związany z działalnością instytucji obowiązanej oraz podejmujący decyzje mające wpływ na to ryzyko (art. 2 ust. 2 pkt 9 u.p.p.p.f.t.). Zaznaczyć należy, iż ani art. 27, ani art. 28 ust. 1 u.p.p.p.f.t. nie precyzują, kto konkretnie ma być odpowiedzialny za przekazywanie oceny ryzyka, wskazana jest jedynie instytucja obowiązana, tym samym osobą uprawnioną do współpracy z GIIF w tym zakresie może być AMLO. Dodatkowo obowiązki wymienione w art. 147 pkt 13 u.p.p.p.f.t. dotyczą już osobiście MLRO. Ważne jest jednak to, że instytucja obowiązana podczas kontroli rozliczana jest ze wszystkich wykonywanych obowiązków określonych w ustawie, dlatego też AMLO zobowiązany jest wykonywać określone czynności zawierające się w procedurze zgodności. Warto jednak zauważyć, że ustawodawca przewidział możliwość wyznaczenia zastępcy AMLO, czyli *Deputy Money Laundering Officer* (DMLO), także w zakresie przekazywania raportów, jednak decyzję w tym zakresie pozostawiono instytucji obowiązanej. Natomiast odpowiedzialność AMLO działającego zarówno jako AMCLO, czy jako MLRO na podstawie art. 8 u.p.p.p.f.t. w zakresie naruszeń z art. 154 ust. 1 u.p.p.p.f.t. nie ulega wątpliwości[51].

[50] https://www.iaml.com.pl/wiedza/kary-sankcje-przeciwdzialanie-praniu-pieniedzy/.

[51] M.A. Kędzierski, *Obowiązki i odpowiedzialność oficera AML (AMLO) w instytucji obowiązanej, cz. 2.*

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

2.5. PODSUMOWANIE

Pranie pieniędzy to zjawisko znane od dawna i jest coraz silniej zwalczane. Legalizacja dochodów z podejrzanych, a czasem ewidentnie przestępczych źródeł, to proceder niewątpliwie szkodliwy dla całej gospodarki. Nic zatem dziwnego, że prawo i różne instytucje publiczne w Polsce, jak i na świecie, coraz silniej starają się takim zjawiskom przeciwdziałać, w wyniku czego ustawodawca nakłada na różnego rodzaju podmioty, które są wskazane w ustawie jako instytucje obowiązane obowiązek przygotowania i przyjęcia wewnętrznych procedur kontroli i zarządzania ryzykiem, przez co konieczne jest wyznaczenie określonych podmiotów, odgrywających określone role w całościowym systemie AML/CFT. Dlatego też w praktyce większe podmioty ze względów organizacyjnych posiadają zarówno AMLO, który ponosi odpowiedzialność za *compliance* oraz kontrolę wewnętrzną, jak i MRLO, który zaś zajmuje się analizą wszelkich wpływających sygnałów, a także oceną i raportowaniem transakcji do GIIF. W takim przypadku najistotniejsze jest ustalenie zakresu czynności AMLO i MRLO, gdyż od tego zależy ich odpowiedzialność. Podstawą odpowiedzialności AMLO jest nie tylko u.p.p.p.f.t., ale także inne akty prawne, choćby takie jak Kodeks pracy[52] czy Prawo bankowe[53]. AMLO będący pracownikiem instytucji obowiązanej, zatrudniony na umowę o pracę, ponosi odpowiedzialność, jak każdy inny pracownik zgodnie z art. 108 k.p., za nieprzestrzeganie ustalonej organizacji i porządku w procesie pracy, przepisów bezpieczeństwa i higieny pracy, przepisów przeciwpożarowych, a także przyjętego sposobu potwierdzania przybycia i obecności w pracy oraz usprawiedliwiania nieobecności w pracy. Za takie naruszenia pracodawca może nałożyć na AMLO karę upomnienia lub nagany. Natomiast nieprzestrzeganie przepisów bezpieczeństwa i higieny pracy lub przepisów przeciwpożarowych, opuszczenie pracy bez usprawiedliwienia, stawienie się do pracy w stanie nietrzeźwości lub spożywanie alkoholu w czasie pracy może skutkować nałożeniem na AMLO kary pieniężnej. Dodatkowo oprócz tego, że AMLO obowiązują przepisy w zakresie kodeksu pracy, to jeśli jest on pracownikiem banku musi przestrzegać także przepisów prawa bankowego, które nakładają na niego określone obowiązki. Zgodnie z art. 107 u.p.b. pracownik, który wbrew swoim obowiązkom nie zawiadamia o okolicznościach wymienionych w art. 106 ust. 1, ponosi odpowiedzialność porządkową, co nie wyłącza odpowiedzialności karnej, jeżeli czyn wypełnia znamiona przestępstwa. W tym przypadku widać, jak istotna jest rola AMLO w zakresie przestrzegania obowiązku przeciwdziałania praniu pieniędzy. Wymiar odpowiedzialności z art. 107 pb w kontekście art. 106 ust. 1 u.p.b. oraz regulacji zawartych w u.p.p.p.f.t. i kodeksie karnym należy uznać raczej za pomocniczy i symboliczny.

[52] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2020 r., poz. 1320), zwana dalej: k.p.

[53] Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. z 1997 r., nr 140, poz. 939), zwana dalej: u.p.b.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Justyna Gryniuk
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 3.

PROBLEMATYKA IDENTYFIKACJI BENEFICJENTA RZECZYWISTEGO

3.1. UWAGI WPROWADZAJĄCE

Geneza przedmiotowego rozdziału, jak i całej monografii wynika ze zmian w regulacji AML, a w szczególności pozostaje w związku z wejściem w życie *U*stawy z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw. Celem rozdziału będzie wskazanie nowych regulacji dotyczących beneficjenta rzeczywistego przy uwzględnieniu zmian, które wejdą w życie z dniem 31 października 2021 r.

Warto również omówić źródło powstania potrzeby identyfikacji beneficjenta rzeczywistego, zarówno prawnej, jak i faktycznej. Ustawa ta ma na celu implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/843 (5AMLD). Jednym z celów dyrektywy jest zwiększenie transparentności informacji o beneficjentach rzeczywistych podmiotów o charakterze korporacyjnym, dlatego warto wskazać przyczynę powstania nowych regulacji prawnych[1]. Szczególnym celem niniejszego rozdziału będzie także wskazanie wymagań stawianych przed instytucjami obowiązanymi, w związku z nowymi regulacjami pojawiły się komplikacje z samym procesem identyfikacyjnym beneficjentów rzeczywistych, w szczególności, zgodnie z art. 34 ust. 1 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, obligatoryjną czynnością poza samą identyfikacją jest podjęcie uzasadnionych czynności celem zweryfikowania tożsamości beneficjenta

[1] Uzasadnienie projektu ustawy o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw, https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=909 (data dostępu: 7 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

rzeczywistego oraz ustalenia struktury własności i kontroli[2]. Podmioty obowiązane muszą wykonać wiele czynności, aby prawidłowo dopełnić tego obowiązku. Celem rozdziału będzie zatem omówienie środków bezpieczeństwa finansowego.

Ponadto przedmiotem badania jest wskazanie podmiotów obowiązanych do zgłaszania swoich beneficjentów rzeczywistych oraz rozwiązań przewidzianych w ustawie, aby należycie dopełnić tego obowiązku. W tym celu istotnym będzie omówienie kwestii Centralnego Rejestru Beneficjentów Rzeczywistych, przede wszystkim, kto jest zobowiązany do jego prowadzenia, weryfikacji oraz zasilania danymi. W tej kwestii wartym będzie wskazanie związku Centralnego Rejestru Beneficjentów Rzeczywistych pomiędzy Krajowym Rejestrem Sądowym. Ponadto w niniejszym rozdziale warto omówić strukturę odpowiedzialności, możliwe kary za niedopełnienie obowiązków zgłoszenia oraz omówienie wymogu niekaralności beneficjentów rzeczywistych.

3.2. KTO JEST UZNAWANY ZA BENEFICJENTA RZECZYWISTEGO?

Zgodnie z art. 2 ust. 1 pkt 1 Terroryzmu ww. ustawy beneficjentem rzeczywistym jest każda osoba fizyczna, która sprawuje bezpośrednio lub pośrednio kontrolę nad klientem poprzez posiadane uprawnienia. Uprawnienia te muszą wynikać z okoliczności prawnych lub faktycznych, umożliwiających wywieranie decydującego wpływu na czynności lub działania podejmowane przez klienta lub przez każdą osobę fizyczną, w imieniu której są nawiązywane stosunki gospodarcze lub przeprowadzana jest transakcja okazjonalna. W przypadku osoby prawnej innej niż spółka, której papiery wartościowe są dopuszczone do obrotu na rynku regulowanym podlegającym wymogom ujawniania informacji wynikającym z przepisów prawa Unii Europejskiej lub odpowiadających im przepisów prawa państwa trzeciego. Za beneficjenta rzeczywistego uważa się osobę fizyczną będącą udziałowcem lub akcjonariuszem, której przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji tej osoby prawnej.

Za beneficjenta rzeczywistego uważa się również osobę fizyczną dysponującą więcej niż 25% ogólnej liczby głosów w organie stanowiącym tej osoby prawnej, również jako zastawnik albo użytkownik, lub na podstawie porozumień z innymi uprawnionymi do głosu, także osobę fizyczną sprawującą kontrolę nad osobą prawną lub osobami prawnymi, którym łącznie przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji, lub które łącznie dysponują więcej niż 25% ogólnej liczby głosów w organie stanowiącym tej osoby prawnej, także jako

[2] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

zastawnik albo użytkownik, lub na podstawie porozumień z innymi uprawnionymi do głosu. Beneficjentem rzeczywistym jest także osoba fizyczna sprawująca kontrolę nad osobą prawną poprzez posiadane uprawnienia, o których mowa w art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2021 r., poz. 217), lub osoba fizyczna zajmującą wyższe stanowisko kierownicze w przypadku udokumentowanego braku możliwości ustalenia lub wątpliwości co do tożsamości osób fizycznych określonych w tiret pierwszym–czwartym oraz w przypadku niestwierdzenia podejrzeń prania pieniędzy lub finansowania terroryzmu. Natomiast w przypadku trustu za beneficjenta uważa się założyciela, powiernika, nadzorcę, jeśli został ustanowiony, beneficjenta lub w przypadku gdy osoby fizyczne czerpiące korzyści z danego trustu nie zostały jeszcze określone, to uważa się grupę osób, w których głównym interesie powstał lub działa trust, a także inną osobę sprawującą kontrolę nad trustem oraz inną osobę fizyczną posiadającą uprawnienia lub wykonującą obowiązki równoważne z określonymi w tiret pierwszym–piątym. Co istotne, w przypadku osoby fizycznej prowadzącej działalność gospodarczą, wobec której nie stwierdzono przesłanek lub okoliczności mogących wskazywać na fakt sprawowania kontroli nad nią przez inną osobę fizyczną lub osoby fizyczne, przyjmuje się, że taka osoba fizyczna jest jednocześnie beneficjentem rzeczywistym[3].

Jednak są sytuacje, w których problematyczne jest ustalenie beneficjenta rzeczywistego. Może być to sytuacja, w której wśród wspólników znajdują się zarówno osoby fizyczne, jak i prawne, a żadna z nich nie przekracza progu 25%. Jakub Zawadzki w swoim artykule pisze: *Pierwszym sposobem postępowania w takiej sytuacji jest „sumowanie" kontroli wykonywanej bezpośrednio i pośrednio. Na przykład, gdy wspólnik posiada we własnym imieniu 20% jednostek danego podmiotu, a jednocześnie kontrolowana przez niego w 60% osoba prawna również posiada 20% jednostek tego samego podmiotu, to dla celów ustalenia beneficjenta rzeczywistego oba udziały należy proporcjonalnie zsumować i przypisać tej osobie fizycznej 32% jednostek spółki podlegającej zgłoszeniu, a w efekcie uznać ją za beneficjenta rzeczywistego.* W artykule tym omawia także drugą możliwość ustalenia beneficjenta rzeczywistego w problematycznej do ustalenia sytuacji: *Inną metodą jest uważne przeanalizowanie dokumentów korporacyjnych podmiotu, w szczególności umowy spółki, umowy wspólników, umowy inwestycyjnej itp., lub odwołanie się do ogólnych przesłanek uznania za beneficjenta rzeczywistego (...)*[4].

[3] *Ibidem*.

[4] J. Zawadzki, *W poszukiwaniu beneficjenta rzeczywistego*, https://www.parp.gov.pl/component/content/article/62251:w-poszukiwaniu-beneficjenta-rzeczywistego (data dostępu: 7 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

3.3. ŚRODKI BEZPIECZEŃSTWA FINANSOWEGO

Stosowanie środków bezpieczeństwa finansowego jest jednym z obowiązków, wynikającym z ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Ku wypełnieniu tego obowiązku istotne jest posiadanie statusu instytucji obowiązanej. Instytucje te wymienione są w art. 2 ust. 1 Terroryzmu. Są to na przykład banki czy podmioty prowadzące biura rachunkowe. Instytucje te są zobowiązane do stosowania wobec swoich klientów środków bezpieczeństwa finansowego, w tym rozpoznania ryzyka prania pieniędzy oraz finansowania terroryzmu związanego ze stosunkami gospodarczymi lub z transakcją okazjonalną. Muszą także ocenić poziom rozpoznanego ryzyka oraz prowadzić dokumentację rozpoznanego ryzyka prania pieniędzy oraz finansowania terroryzmu, związanego ze stosunkami gospodarczymi lub z transakcją okazjonalną[5].

Natomiast w kwestii beneficjenta rzeczywistego, zgodnie z art. 34. 1 Terroryzmu, środki bezpieczeństwa finansowego dotyczą jego identyfikacji, podjęcia uzasadnionych czynności celem weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli. Zweryfikowanie beneficjenta rzeczywistego w pewnych sytuacjach jest niemożliwe, dlatego też aby dopełnić obowiązku odpowiednio zastosowanego środka bezpieczeństwa istotny jest fakt samego podjęcia uzasadnionych czynności, na przykład sprawdzenia w tym celu dostępnych rejestrów[6]. Instytucje obowiązane także dokonują oceny stosunków gospodarczych, oraz stosownie do sytuacji uzyskują informacje na temat celu i zamierzonego charakteru tych stosunków. Mogą one także powierzyć realizację tych środków podmiotowi trzeciemu. Podmiotem takim, zgodnie z art. 47 ust. 3 Terroryzmu może być *instytucja obowiązana, podmiot z siedzibą w innym państwie lub organizacja członkowska lub federacja zrzeszająca taki podmiot, który na podstawie właściwych przepisów tego państwa z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu jest obowiązany do stosowania środków bezpieczeństwa finansowego i przechowywania dokumentów i informacji oraz podlega nadzorowi właściwych organów tego państwa w sposób odpowiadający wymogom wynikającym z przepisów Unii Europejskiej z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu*[7]. Istotnym jest, że instytucje nie mogą korzystać z usług podmiotu, mającego siedzibę w państwie trzecim wysokiego ryzyka. Jednakże na podstawie art. 47 ust 4 Terroryzmu zakaz ten nie obowiązuje w przypadkach korzystania z usług *oddziałów instytucji obowiązanych lub jednostek zależnych z większościowym*

[5] K.J. Musiał, *Środki bezpieczeństwa finansowego,* https://sip.lex.pl/procedury/srodki-bezpieczenstwa-finansowego-1610618975 (data dostępu: 7 lipca 2021).

[6] A.J. Szereda, *Notariat. Czynności Notarialne. Wydanie I. Środki bezpieczeństwa finansowego*, C.H. Beck, Warszawa 2021, s. 3.

[7] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

udziałem instytucji obowiązanych, oddziałów lub jednostek zależnych z większościowym udziałem podmiotów mających siedzibę na terytorium państwa członkowskiego oraz podlegających obowiązkom wynikającym z przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, wydanych na podstawie dyrektywy 2015/849 – jeżeli stosują procedury grupowe, o których mowa w art. 51 ust. 1[8]. Zgodnie z art. art. 47 ust 1 Terroryzmu, podmiot trzeci jest zobowiązany do niezwłocznego przekazywania kopii dokumentów o zastosowanych środkach w kwestii identyfikacji beneficjenta rzeczywistego i weryfikacji jego tożsamości, na każde żądanie instytucji. Począwszy od dnia 31 października 2021 r. przepis ten będzie stanowił także o możliwości dostarczania informacji przez te podmioty „za pomocą środków identyfikacji elektronicznej oraz usług zaufania umożliwiających identyfikację elektroniczną w rozumieniu rozporządzenia 910/2014”[9]. Co istotne, na gruncie art. 47 ust. 2 Terroryzmu, korzystanie z usług podmiotu trzeciego nie będzie zwalniało z odpowiedzialności za zastosowane środki.

3.4. IDENTYFIKACJA BENEFICJENTA RZECZYWISTEGO

Zgodnie z Ustawą, z dnia 1 marca 2018 r. wprowadzony został w szczególności obowiązek zgłaszania informacji o beneficjentach rzeczywistych[10]. Identyfikacja beneficjenta rzeczywistego następuje poprzez ustalenie imienia i nazwiska oraz obywatelstwa, a w przypadku posiadania informacji przez instytucję obowiązaną również ustalenie numeru PESEL lub daty urodzenia, w sytuacji w której nie nadano numeru PESEL, państwa urodzenia, serii i numeru dokumentu stwierdzającego tożsamość osoby oraz adresu zamieszkania w przypadku posiadania tej informacji przez instytucję obowiązaną. Jednak zgodnie z nowym brzmieniem artykułu, który wejdzie w życie dnia 31 października 2021 r. nastąpi zmiana co do danych, wtedy identyfikacja beneficjenta rzeczywistego obejmie ustalenie tylko imienia i nazwiska, a w przypadku posiadania informacji przez instytucję obowiązaną zostanie dodany także obowiązek ustalenia obywatelstwa[11]. W przypadku osób prowadzących działalność gospodarczą, koniecznym jest ustalenie nazwy (firmy),

[8] *Ibidem*.

[9] Nowe brzmienie ust. 1 w art. 47 wejdzie w życie z dniem 31 października 2021 r. (t.j. Dz.U. z 2021 r., poz. 815).

[10] K.J. Musiał, *Zgłaszanie informacji o beneficjentach rzeczywistych,* https://sip.lex.pl/procedury/zglaszanie-informacji-o-beneficjentach-rzeczywistych-1610618941 (data dostępu: 7 września 2021).

[11] Art. 36 ust. 2 w zw. ust. 1 pkt 1 a–e (t.j. Dz.U. z 2018 r., poz. 723).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

numeru identyfikacji podatkowej (NIP) oraz adresu głównego miejsca wykonywania działalności gospodarczej[12].

Zweryfikowanie tożsamości beneficjenta rzeczywistego następuje poprzez potwierdzenie ustalonych danych identyfikacyjnych na podstawie dokumentu stwierdzającego tożsamość osoby fizycznej, dokumentu zawierającego aktualne dane z wyciągu z właściwego rejestru lub innych dokumentów, danych lub informacji pochodzących z wiarygodnego i niezależnego źródła. W tej kwestii od dnia 31 października 2021 r. nastąpi zmiana i będzie to także możliwe poprzez identyfikację elektroniczną. W przypadku identyfikacji beneficjenta rzeczywistego, instytucje obowiązane dokumentują wszelkie utrudnienia, które spowodowały brak możliwości ustalenia tożsamości osób fizycznych lub wątpliwości co do ich tożsamości. Co istotne, instytucje obowiązane stosując środki bezpieczeństwa finansowego nie będą polegać wyłącznie na informacjach wynikających z Centralnego Rejestru Beneficjentów Rzeczywistych lub rejestru, o którym mowa w art. 30 lub art. 31 dyrektywy Parlamentu Europejskiego i Rady 2015/849[13–14]. Tożsamość beneficjenta rzeczywistego zostaje zweryfikowana przed nawiązaniem stosunków gospodarczych lub przed przeprowadzeniem transakcji okazjonalnej. Jednak, jeżeli zachodzi przesłanka zachowania ciągłości prowadzenia działalności gospodarczej oraz występuje niskie ryzyko prania pieniędzy i finansowania terroryzmu, wówczas weryfikacja beneficjenta rzeczywistego może być zakończona podczas nawiązywania stosunków gospodarczych, w takim przypadku weryfikacja ta musi być dokonana w możliwie jak najkrótszym terminie od momentu rozpoczęcia nawiązywania stosunków gospodarczych. Instytucje obowiązane, na przykład banki[15], mogą zawrzeć umowę o prowadzenie rachunku bankowego, rachunku papierów wartościowych lub rachunku zbiorczego, jednak przed przeprowadzeniem transakcji, zaś z wykorzystaniem tych rachunków muszą zastosować środki bezpieczeństwa finansowego. Co więcej, w przypadku trustów, na gruncie art. 39 Terroryzmu, instytucje obowiązane uzyskują informacje dotyczące rodzaju tych beneficjentów, aby umożliwić identyfikację beneficjenta w momencie dokonywania wypłaty wartości majątkowych lub wykonywania przez beneficjenta przysługujących mu praw.

Natomiast w przypadku nawiązywania stosunków gospodarczych lub przeprowadzania transakcji okazjonalnej z podmiotem podlegającym obowiązkowi rejestracji informacji o beneficjentach rzeczywistych instytucje obowiązane uzyskują

[12] A.J. Szereda, *op. cit*., s. 3.

[13] Na podstawie art. 30 lub art. 31 Dyrektywy Parlamentu Europejskiego i Rady 2015/849 mowa w szczególności o rejestrze handlowym lub rejestrze spółek

[14] Nowe brzmienie art. 37 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[15] Wszystkie instytucje, których dotyczy ten obowiązek zawarte są w katalogu w art. 2 ust. 1 pkt 1–5, 7–11, 24 i 25 Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

potwierdzenie rejestracji albo odpis z Centralnego Rejestru Beneficjentów Rzeczywistych lub rejestru prowadzonego we właściwym państwie członkowskim. Podmioty te są zobowiązane do udostępniania informacji i dokumentów, które pozwalają na identyfikację tożsamości ich beneficjentów rzeczywistych[16].

Co do zasady, środki bezpieczeństwa są stosowane w sytuacjach, w których wartość transakcji okazjonalnej przekracza kwotę 15 000 euro, wliczając wartość transakcji z nią powiązanych lub jeżeli wartość transakcji gotówkowej przekracza kwotę 10 000 euro, również wliczając powiązane z nią transakcje. Jednak środki bezpieczeństwa finansowego stosuje się też bez względu na wielkość wartości transakcji, ponieważ także w sytuacjach, w których nastąpi samo podejrzenie ryzyka prania pieniędzy lub finansowania terroryzmu[17].

3.5. OSOBY ZAJMUJĄCE EKSPONOWANE STANOWISKA POLITYCZNE

Instytucje na podstawie art. 46 Terroryzmu mają również obowiązek zweryfikowania na podstawie dostępnych źródeł, czy dana osoba nie jest osobą zajmującą eksponowane stanowisko polityczne. W tym celu instytucje zobowiązane są do zastosowania procedury opartej na analizie ryzyka. Procedurą taką będzie przyjęcie od klienta oświadczenia, że jest on lub nie jest osobą zajmującą takie stanowisko, takie oświadczenie jest składane pod rygorem odpowiedzialności karnej na podstawie art. 233 § 6 Kodeksu karnego[18]. Składający oświadczenie musi zawrzeć w nim klauzulę, że jest świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia, warto wskazać, iż zgodnie z art. 46 ust. 1 Terroryzmu, jest to zastąpieniem pouczenia o odpowiedzialności karnej za złożenie fałszywego oświadczenia. Kogo zatem w świetle ustawy można uznać za osobę zajmującą eksponowane stanowisko polityczne? W tym przypadku nie dotyczy to grup stanowisk średniego i niższego szczebla. Ustawa stanowi, że takimi osobami są osoby zajmujące znaczące stanowiska publiczne lub pełniące znaczące funkcje publiczne. Ustawodawca wymienia te podmioty w katalogu w art. 2 ust. 2 pkt 11 i są to kolejno: *szefowie państw, szefowie rządów, ministrowie, wiceministrowie oraz sekretarze stanu, członkowie parlamentu lub podobnych organów ustawodawczych, członkowie organów zarządzających partii politycznych, członkowie sądów najwyższych, trybunałów konstytucyjnych i innych organów sądowych wysokiego szczebla, których decyzje nie podlegają zaskarżeniu, z wyjątkiem trybów nadzwyczajnych, członkowie trybunałów obrachunkowych lub zarządów banków central-*

[16] Ust. 1a w art. 39 wejdzie w życie dnia 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).
[17] A.J. Szereda, *op. cit.*, s. 3.
[18] *Ibidem*, s. 13.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nych, ambasadorzy, chargés d'affaires oraz wyżsi oficerowie sił zbrojnych, członkowie organów administracyjnych, zarządczych lub nadzorczych przedsiębiorstw państwowych, spółek z udziałem Skarbu Państwa, w których ponad połowa akcji albo udziałów należy do Skarbu Państwa lub innych państwowych osób prawnych, dyrektorzy, zastępcy dyrektorów oraz członków organów organizacji międzynarodowych lub osoby pełniące równoważne funkcje w tych organizacjach, dyrektorzy generalni w urzędach naczelnych i centralnych organów państwowych oraz dyrektorzy generalni urzędów wojewódzkich i inne osoby zajmujące stanowiska publiczne lub pełniące funkcje publiczne w organach państwa lub centralnych organach administracji rządowej[19].

Instytucje w sytuacji istnienia stosunków gospodarczych z osobą zajmującą eksponowane stanowisko polityczne zobowiązane są do zastosowania środków bezpieczeństwa finansowego, w tym ustalenia źródła majątku oraz źródła pochodzenia majątku, którym dysponuje w ramach stosunków gospodarczych, np. w przypadku notariuszy, poprzez przyjęcie oświadczenia, że jego majątek pochodzi z legalnego źródła[20]. Obok innych środków bezpieczeństwa finansowego, instytucje muszą uzyskać również zgodę kadry kierowniczej wyższego szczebla na nawiązanie albo kontynuację stosunków gospodarczych z osobą zajmującą eksponowane stanowisko polityczne.

Zgodnie z art. 2 ust. 1 pkt 8 Terroryzmu instytucje takie jak zakłady ubezpieczeń, które są stroną umowy ubezpieczenia, zobowiązane są do podjęcia odpowiednich środków w związku z art. 46 ust. 3 Terroryzmu ku ustaleniu, czy beneficjenci rzeczywiści uprawnieni z tytułu umowy są osobami zajmującymi eksponowane stanowiska polityczne. Natomiast w sytuacji, kiedy zostanie stwierdzone wyższe ryzyko prania pieniędzy lub finansowania terroryzmu, instytucje te są zobowiązane do zastosowania środków bezpieczeństwa finansowego przed wypłatą świadczenia z tytułu umowy ubezpieczenia lub przeniesienia praw z tytułu umowy ubezpieczenia. W tym celu zgodnie z art. 46 ust. 4 Terroryzmu muszą także dokonać pogłębionej analizy stosunków gospodarczych z klientem oraz informować o zamiarze wypłaty tego świadczenia kadrę kierowniczą wyższego szczebla. Zgodnie z art. 46 ust. 5 Terroryzmu, instytucja jest zobowiązana do zastosowania środków uwzględniających wyższe ryzyko, nawet w sytuacji zaprzestania zajmowania przez osobę eksponowanego stanowiska politycznego. W tej sytuacji wyższe ryzyko występuje także od dnia zaprzestania zajmowania eksponowanego stanowiska politycznego, aż do dnia ustalenia, że z tą osobą nie wiąże się już ryzyko. Nie może to jednak nastąpić krócej niż przez okres 12 miesięcy.

W tym miejscu warto także zwrócić uwagę, iż wspomniane przepisy stanowią także o konieczności stosowania ich co do członków rodziny osoby zajmującej

[19] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723).

[20] A.J. Szereda, *op. cit*., s. 14.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

eksponowane stanowisko oraz bliskich współpracowników[21]. Należy zatem wskazać zgodnie z art. 2 ust. 2 pkt 3 Terroryzmu, że za członków rodziny osoby zajmującej eksponowane stanowisko polityczne uważa się małżonka lub osobę pozostającą we wspólnym pożyciu z tą osobą, jego dziecko oraz dziecko małżonka lub osoby pozostającej we wspólnym pożyciu. Co istotne, na gruncie art. 2 ust. 2 pkt 12 Terroryzmu, za znanych jako bliskich współpracowników osoby zajmującej eksponowane stanowisko polityczne uważa się osoby fizyczne będące beneficjentami rzeczywistymi osób prawnych, jednostek organizacyjnych nieposiadających osobowości prawnej lub trustów wspólnie z osobą zajmującą eksponowane stanowisko polityczne lub utrzymujące z taką osobą inne bliskie stosunki związane z prowadzoną działalnością gospodarczą oraz osoby fizyczne będące jedynym beneficjentem rzeczywistym osób prawnych, jednostek organizacyjnych nieposiadających osobowości prawnej lub trustu, o których wiadomo, że zostały utworzone w celu uzyskania faktycznej korzyści przez osobę zajmującą eksponowane stanowisko polityczne.

Natomiast od 31 października 2021 r. wejdzie w życie przepis, nakładający obowiązek na Generalnego Inspektora, stanowiący o przekazywaniu Komisji Europejskiej wykazu krajowych stanowisk oraz funkcji publicznych będących eksponowanymi stanowiskami politycznymi, w tym przypadku według art. 2 ust. 2 pkt 11 lit. a–g, i, j Terroryzmu dotyczy to: *szefów państw, szefów rządów, ministrów, wiceministrów oraz sekretarzy stanu, członków parlamentu lub podobnych organów ustawodawczych, członków organów zarządzających partii politycznych, członków sądów najwyższych, trybunałów konstytucyjnych oraz innych organów sądowych wysokiego szczebla, których decyzje nie podlegają zaskarżeniu, z wyjątkiem trybów nadzwyczajnych, członków trybunałów obrachunkowych lub zarządów banków centralnych, ambasadorów, chargés d'affaires oraz wyższych oficerów sił zbrojnych, członków organów administracyjnych, zarządczych lub nadzorczych przedsiębiorstw państwowych, spółek z udziałem Skarbu Państwa, w których ponad połowa akcji albo udziałów należy do Skarbu Państwa lub innych państwowych osób prawnych oraz innych osób zajmujących stanowiska publiczne lub pełniące funkcje publiczne w organach państwa lub centralnych organach administracji rządowej*[22].

Ponadto wydane zostanie rozporządzenie ministra właściwego do spraw finansów publicznych. Nastąpi w nim określenie wykazu krajowych stanowisk i funkcji publicznych wymienionych powyżej, zważywszy na charakter wykonywanych zadań i znaczenie dla przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

[21] Art. 46 ust. 6, Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723).

[22] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Zgodnie z art. 2 ust. 2 pkt 11 lit. h. Terroryzmu, organizacje międzynarodowe mające siedzibę w Polsce będą przekazywać oraz mogą podawać do publicznej wiadomości poprzez stronę internetową wykaz aktualnych stanowisk i funkcji w organizacjach międzynarodowych będących eksponowanymi stanowiskami politycznymi. tj. dyrektorów, zastępców dyrektorów oraz członków organów organizacji międzynarodowych lub osób pełniących równoważne funkcje w tych organizacjach.

Instytucje muszą mieć wprowadzoną wewnętrzną procedurę dotyczącą przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Są one zobowiązane do bieżącej weryfikacji i aktualizacji danych, przy uwzględnieniu charakteru, rodzaju oraz rozmiaru prowadzonej działalności. Procedura wewnętrzna *musi określać zasady odnotowywania rozbieżności między informacjami zgromadzonymi w Centralnym Rejestrze Beneficjentów Rzeczywistych a informacjami o beneficjentach rzeczywistych klienta ustalonymi w związku ze stosowaniem ustawy*[23]. Procedura ta, powinna określać *zasady dokumentowania utrudnień stwierdzonych w związku z weryfikacją tożsamości beneficjenta rzeczywistego oraz czynności podejmowanych w związku z identyfikacją jako beneficjenta rzeczywistego osoby fizycznej zajmującej wyższe stanowisko kierownicze*[24]. Wprowadzenie oraz aktualizowanie wewnętrznej procedury musi zostać zaakceptowane przez kadrę kierowniczą wyższego szczebla[25].

3.6. CENTRALNY REJESTR BENEFICJENTÓW RZECZYWISTYCH

Centralny Rejestr Beneficjentów Rzeczywistych (dalej jako: CRBR) służy do przetwarzania informacji o beneficjentach rzeczywistych. Dotyczy on obowiązku zgłaszania oraz aktualizacji informacji o beneficjentach rzeczywistych spółek jawnych, spółek komandytowych, spółek komandytowo-akcyjnych, spółek z ograniczoną odpowiedzialnością, prostych spółek akcyjnych, spółek akcyjnych z wyłączeniem spółek publicznych[26]. Gromadzone są w nim dokładne i aktualne dane o beneficjen-

[23] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 50 ust. 2 pkt 10 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[24] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 50 ust. 2 pkt 11 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[25] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 50 ust. 3 nowe brzmienie ust. 3 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[26] Spółki publiczne – w rozumieniu ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (Dz.U. z 2020 r., poz. 2080 oraz z 2021 r., poz. 355).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

tach rzeczywistych. CRBR ma za zadanie wspierać zwalczanie prania pieniędzy i finansowania terroryzmu, ponieważ docelowo służy on uniemożliwianiu przestępcom ukrycia swojej tożsamości[27].

Zgodnie z nowelizacją Ustawy, z dniem 31 października 2021 r. do podmiotów obowiązanych dołączą także trusty, których powiernicy lub osoby zajmujące stanowiska równoważne mają miejsce zamieszkania lub siedzibę na terytorium Rzeczypospolitej Polskiej lub nawiązują stosunki gospodarcze albo nabywają nieruchomość na terytorium Rzeczypospolitej Polskiej w imieniu lub na rzecz trustu. Do podmiotów tych dołączą także spółki partnerskie, europejskie zgrupowania interesów gospodarczych, spółki europejskie, spółdzielnie, spółdzielnie europejskie, stowarzyszenia podlegające wpisowi do Krajowego Rejestru Sądowego oraz fundacje[28]. Do rejestru podmioty obowiązane zgłaszają dane identyfikacyjne dotyczące beneficjenta rzeczywistego, tj. imię i nazwisko, obywatelstwo, państwo zamieszkania, numer PESEL lub datę urodzenia, dotyczy osób nieposiadających numeru PESEL, oraz informacje o wielkości i charakterze udziału albo informacje o uprawnieniach, które przysługują beneficjentowi rzeczywistemu. Zgodnie z nowelizacją obowiązek informacyjny dotyczyć będzie każdego posiadanego obywatelstwa[29].

Ponadto wraz z nowelizacją, zostanie dodany pkt 3 w art. 59, stanowiący o obowiązku informacyjnym dotyczącym danych beneficjenta rzeczywistego trustu. Obowiązek ten będzie obejmował dane, takie jak: imię i nazwisko, każde posiadane obywatelstwo, państwo zamieszkania, numer PESEL lub datę urodzenia w przypadku jego braku, informację o uprawnieniach przysługujących beneficjentowi rzeczywistemu w przypadku trustu[30], oraz obowiązek o zawarciu informacji o grupie osób, w których głównym interesie powstał lub działa trust[31].

Termin na zgłoszenie powyższych informacji wynosi nie więcej niż siedem dni od dnia wpisania spółki do KRS. Natomiast jeżeli nastąpiła zmiana w przekazanych informacjach, w terminie siedmiu dni od ich zmiany. Natomiast od dnia

[27] A. Hołda, *Instrukcje księgowe i podatkowe. Rozdział I. Wewnętrzna procedura instytucji obowiązanej oraz zgłoszenie beneficjenta rzeczywistego do CRBR*, wyd. 2, C.H. Beck, Warszawa 2020, s. 7.

[28] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 58 dodane pkt 6–13 w art. 58 wejdą w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[29] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Nowe brzmienie wprow. do wyliczenia oraz lit. b w pkt 2 w art. 59 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[30] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Beneficjent rzeczywisty w przypadku trustu – definicja zawarta w art. 2 ust. 2 pkt 1 lit. b tiret czwarte.

[31] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Dodany punkt 3 w art. 59 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

31 października 2021 r. podmioty zobowiązane z wyłączeniem trustu informacje te muszą zgłosić w terminie siedmiu dni od dnia wpisu tych podmiotów do KRS. W sytuacji dokonywania aktualizacji danych, termin ten również będzie wynosił siedem dni od ich zmiany danych w KRS, ale jeżeli nastąpi zmiana, która nie skutkuje potrzebą wpisu do KRS, to termin ten będzie wynosił siedem dni od dnia dokonania tych zmian.

W przypadku trustu należy zgłosić wymienione informacje, również w terminie siedmiu dni, ale liczonego od dnia *utworzenia trustu, przeniesienia siedziby lub miejsca zamieszkania na terytorium Rzeczypospolitej Polskiej przez powiernika trustu lub osobę zajmującą równoważne stanowisko oraz od dnia nawiązania stosunków gospodarczych lub nabycia nieruchomości na terytorium Rzeczypospolitej Polskiej, w imieniu lub na rzecz trustu, przez powiernika trustu lub osobę zajmującą równoważne stanowisko*[32]. Ponadto w przypadku trustu warto wskazać na obowiązek aktualizowania informacji zgłaszanych do rejestru w czasie utrzymywania stosunków gospodarczych na terytorium Rzeczypospolitej Polskiej. Obowiązek aktualizacji dotyczy także okresu, w którym powiernik lub osoba zajmująca równoważne stanowisko, działająca w imieniu albo na rzecz trustu, posiada nieruchomość lub jest jej właścicielem na terytorium Rzeczypospolitej Polskiej[33].

Natomiast zmiana w przypadku aktualizacji informacji musi zostać zgłoszona w terminie siedmiu dni od dnia dokonania tej zmiany. Do wymienionych terminów nie wlicza się sobót ani dni ustawowo wolnych od pracy[34]. Jak przedstawia się natomiast sytuacja w przypadku wystąpienia awarii funkcjonowania rejestru? Ustawa w artykule 60 ust. 3 wskazuje rozwiązanie w takiej sytuacji, także omawiając kwestię biegu terminu: *W przypadku awarii lub zakłóceń funkcjonowania systemu teleinformatycznego organ właściwy w sprawach rejestru informuje o ich wystąpieniu i usunięciu w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych. W takim przypadku do biegu terminów, o których mowa w ust. 1 i 1a, nie wlicza się okresu od chwili wystąpienia awarii lub zakłócenia wskazanych w informacji zamieszczonej w tym Biuletynie do chwili zamieszczenia informacji o ich usunięciu*[35].

[32] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 60 ust. 1 w zw. z art. 60 ust. 1a dodany ust. 1a wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[33] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 60 ust. 1b dodany ust. 1b wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[34] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 60 ust. 2 zmiany w ust. 2 art. 60 wejdą w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[35] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 60 ust. 3, zmiana ust. 3 w art. 60 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Na beneficjencie rzeczywistym spoczywa obowiązek dostarczenia powyżej wymienionym spółkom, w przypadku trustu – powiernikowi lub osobie zajmującej stanowisko równoważne, wszelkich informacji i dokumentów, które potrzebne są do zgłaszania oraz aktualizowania informacji, zgodnie z terminem zgłoszenia ich do rejestru[36]. Zgłoszenia dokonują organy reprezentacyjne spółek, w przypadku trustu – powiernik lub osoba zajmująca stanowisko równoważne. Dokonując zgłoszenia, należy zawrzeć dane, takie jak: imię i nazwisko, obywatelstwo, miejsce zamieszkania, numer PESEL lub datę urodzenia w przypadku jego braku. W tym celu podaje także swoją funkcję, uprawniającą go do zgłoszenia. Zgłoszenie jest nieodpłatne oraz dokonuje się go w formie elektronicznej za pomocą wzoru dokumentu dostępnego w Centralnym Repozytorium Wzorów Dokumentów Elektronicznych o numerze 2019/08/22/8410[37]. Dane, które zgłaszane są do rejestru, powinny odpowiadać rzeczywistości. Zgłoszenie opatrzone jest kwalifikowanym podpisem elektronicznym lub potwierdzonym profilem zaufanym ePUAP. Zawiera oświadczenie osoby, która dokonuje zgłoszenia, że wprowadzone dane są prawdziwe, składane pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia[38].

Co istotne w kwestii CRBR, instytucja obowiązana powinna odnotowywać sprzeczności w informacjach zamieszczonych w rejestrze a ustalonymi informacjami o beneficjencie rzeczywistym, w tym celu jest zobowiązana do podjęcia czynności celem wyjaśnienia przyczyny tych różnic. Natomiast jeżeli rozbieżności te zostaną potwierdzone, wówczas instytucje te są zobowiązane przekazać organowi właściwemu – GIIF, weryfikację, uzasadnienie oraz wszelką dokumentacją dotyczącą odnotowanej rozbieżności. Organ właściwy będzie mógł w tym przypadku wszcząć postępowanie celem wyjaśnienia, czy zamieszczone informacje w rejestrze są prawidłowe i aktualne[39]. GIIF w tym celu może wydać decyzje o sprostowaniu tych danych w rejestrze.

Ponadto, wszelkie niezbędne dane dotyczące wymienionych spółek, z wyjątkiem trustu, przechowywane są przez okres 10 lat liczonego od dnia ich wykreślenia z KRS. Natomiast w przypadku trustu informacje przechowywane są przez 10 lat, ale licząc od dnia, w którym zakończył się obowiązek zgłoszenia danych lub

[36] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Dodany art. 60a wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[37] Ministerstwo Finansów, *Zgłoszenie informacji o beneficjentach*, https://www.gov.pl/web/finanse/zgloszenie-informacji-o-beneficjentach (data dostępu: 7 września 2021).

[38] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Art. 61, nowe brzmienie ust. 1 i dodany ust. 1a w art. 61 wejdą w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[39] S. Milczanowski, K. Sałdan, *Co się zmieni w obowiązku identyfikacji beneficjentów rzeczywistych?*, https://www.dzp.pl/blog/compliance/co-sie-zmieni-w-obowiazku-identyfikacji-beneficjentow-rzeczywistych/ (data dostępu: 8 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ich aktualizacji do rejestru[40]. Istotnym jest, że osoba, która dokonuje zgłoszenia lub aktualizacji danych w rejestrze, ponosi odpowiedzialność za szkodę wyrządzoną zgłoszeniem do rejestru nieprawdziwych danych. Co więcej, odpowiada także w przypadku niezgłoszenia danych oraz ich zmian w ustawowym terminie. Dodatkowo możliwe jest nałożenie kary pieniężnej na beneficjenta rzeczywistego w sytuacji niedopełnienia obowiązku w wysokości do 50 000 zł[41], jednak nie ponosi on odpowiedzialności w sytuacjach, jeżeli szkoda nastąpiła wskutek działania siły wyższej albo z wyłącznej winy poszkodowanego lub osoby trzeciej, za którą osoba zobowiązana do dokonania i aktualizacji informacji nie ponosi odpowiedzialności[42].

3.7. WYMÓG NIEKARALNOŚCI BENEFICJENTA RZECZYWISTEGO

Podmioty, które świadczą usługi wymiany walut pomiędzy walutami wirtualnymi a fiducjarnymi, mają obowiązek uzyskania rejestracji lub zezwolenia. Ustawa wprowadziła Rozdział 11a, regulujący zgodnie z art. 2 ust. 1 pkt 16 Terroryzmu, działalność na rzecz trustów lub spółek oraz na podstawie art. 2 ust. 1 pkt 12 Terroryzmu, dotyczący walut wirtualnych. Zgodnie z dyrektywą, jest to podyktowane potrzebą przeciwdziałania sytuacjom w których ukrywane jest pochodzenie transferów oraz wykorzystuje się anonimowość, jaką oferują takie platformy[43].

Rozdział 11a Terroryzmu stanowi, że działalność ta jest regulowana oraz wymaga wpisu do odpowiedniego rejestru. Istotnym jest, że podmiot, który prowadzi działalność na rzecz spółek albo trustów lub podmiot prowadzący działalność w zakresie walut wirtualnych może podlegać karze pieniężnej w wysokości 100 000 zł, jeżeli nie dopełnił obowiązku uzyskania wpisu do odpowiedniego reje-

[40] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 poz. 723). Nowe brzmienie art. 64 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[41] Nowelizacja ustawy AML dotycząca implementacji Dyrektywy V AML, *Jakie zmiany przyniosła nowelizacja ustawy AML z 2021 roku, związana z implementacją Dyrektywy V AML*?, https://www.iaml.com.pl/wiedza/nowelizacja-ustawy-aml-implementacja-dyrektywy-v-aml/ (data dostępu: 8 września 2021).

[42] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. (t.j. Dz.U. z 2018 r., poz. 723). Nowe brzmienie art. 68 wejdzie w życie z dniem 31 października 2021 r. (Dz.U. z 2021 r., poz. 815).

[43] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

stru[44]. Zgodnie z wchodzącym art. 129 a ust. 2 Terroryzmu, obowiązek uzyskania wpisu nie obejmuje w szczególności radców prawnych czy adwokatów.

Co istotne, również wchodzący art. 129 b ust. 1 oraz art. 129 n. ust. 1 Terroryzmu, stanowi, że prowadzący działalność na rzecz spółek lub trustów oraz wykonujący działalność w zakresie walut wirtualnych nie może być prawomocnie skazany za umyślne przestępstwo w szczególności przeciwko działalności instytucji państwowych oraz samorządu terytorialnego, przeciwko wymiarowi sprawiedliwości, przeciwko wiarygodności dokumentów, przeciwko mieniu, przeciwko obrotowi gospodarczemu i interesom majątkowym w obrocie cywilnoprawnym, przeciwko obrotowi pieniędzmi i papierami wartościowymi, przestępstwo popełnione w celu osiągnięcia korzyści majątkowej lub osobistej, lub umyślne przestępstwo skarbowe. Wymóg ten dotyczy także osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej, a dokładniej, wspólników tych podmiotów prowadzących sprawy spółki lub reprezentujących je oraz dotyczy także członków zarządu.

Zgodnie z art. 129 b ust. 1 pkt 2 w związku art. 129n. ust 1. pkt 2 Terroryzmu wymóg ten dotyczy podmiotów, którym spółka powierzyła prowadzenie spraw spółki czy reprezentację osób będących członkami zarządu oraz na gruncie art. 129 ust. 2 Terroryzmu wymóg niekaralności dotyczy także *osób kierujących wykonywaniem czynności związanych z prowadzeniem działalności na rzecz spółek lub trustów oraz beneficjenta rzeczywistego podmiotu prowadzącego taką działalność.*

Zgodnie z art. 129 ust. 1a Terroryzmu osoby fizyczne będące beneficjentami rzeczywistymi muszą posiadać wiedzę lub doświadczenie w kwestii prowadzonej działalności. Ten warunek zostanie spełniony w przypadku ukończenia szkolenia albo kursu z zakresu wykonywania takich usług bądź wykonywania przez rok czynności związanych ze świadczeniem tych usług[45]. Przedsiębiorca musi wykazać, przedstawiając stosowny dokument, że zakończył kurs, lub wykazać, że przez co najmniej rok wykonywał czynności w zakresie tych usług. Za niespełnienie tego zobowiązania może zostać nałożona kara w wysokości 10 000 zł[46].

[44] M. Bartosiewicz, *AML: znaczące zmiany zbliżają się wielkimi krokami,* https://www.rp.pl/prawo-w-firmie/art8656781-aml-znaczace-zmiany-zblizaja-sie-wielkimi-krokami (data dostępu: 13 września 2021).

[45] K. Majewski, *Zmiany w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,* „Monitor Prawa Bankowego" 2020, nr 1.

[46] A. Hołda*, op. cit.*, s. 9.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

3.8. PODSUMOWANIE

Reasumując należy zauważyć, iż Dyrektywa UE wprowadziła wiele nowych regulacji, aby korzystniej wpływać na walkę z przestępczością finansową. Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu jest wyrazem implementacji tych rozwiązań w Polsce.

Najistotniejszą zmianą jest wprowadzenie Centralnego Rejestru Beneficjentów Rzeczywistych, zapewniającego pewną przejrzystość i dostęp do danych. Zgodnie z dyrektywą ma on za zadanie działać prewencyjnie na potencjalnych przestępców finansowych, ponieważ rejestr ten jest skutecznym środkiem zapewniającym informacje o tożsamości posiadaczy rachunków bankowych i płatniczych oraz ich beneficjentów[47].

Zgodnie z dyrektywą państwa-członkowie są zobowiązane, aby podmioty o charakterze korporacyjnym posiadały odpowiednie, dokładne oraz aktualne dane o ich beneficjentach rzeczywistych, ma to kluczowe znaczenie dla śledzenia przestępców, którzy w przeciwnej sytuacji mogliby swą tożsamość ukrywać za strukturą przedsiębiorstwa.

Regulacje prawne dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu ulegają częstej modyfikacji, jest to z pewnością wyrazem dynamicznie rozwijającej się rzeczywistości, w szczególności możliwości dotyczących walut wirtualnych. W dyrektywie wskazana jest powszechność wykorzystywania sieci walut wirtualnych, mających na celu ukrywanie pochodzenia tych transferów, sieć ta jest gwarantem anonimowości, dlatego też koniecznym stało się rozszerzenie zakresu stosowania dyrektywy (UE) 2015/849, która objęła regulacjami podmioty zajmujące się świadczeniem usług wymiany walut.

Celem niniejszego rozdziału było ujęcie problematyki identyfikacji beneficjenta rzeczywistego. Zostały zatem wskazane środki bezpieczeństwa finansowego, przysługujące instytucjom obowiązanym, jednak z uwagi na obszerność tematu, warte dalszej analizy pozostaje szeroko rozumiana ocena ryzyka, z uwzględnieniem jego czynników.

Przedmiotem rozważań był także wymóg dotyczący niekaralności beneficjentów rzeczywistych. W tej kwestii zostały zatem wymienione przestępstwa za które beneficjent rzeczywisty nie może być prawomocnie skazany. Punktem szczegółowej analizy był również obowiązek dotyczący instytucji obowiązanych, aby weryfikować, czy dana osoba, z którą mają do czynienia, nie jest osobą zajmującą eksponowane stanowisko polityczne, nastąpiło zatem wskazanie, jakie czynności muszą wykonać, aby dopełnić obowiązku na podstawie procedury opartej analizie ryzyka.

[47] C. Martysz, K. Walczak, *Zarys problematyki przeciwdziałania przestępstwom gospodarczym i ich wykrywania*, Szkoła Główna Handlowa w Warszawie, Warszawa 2018, s. 9.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Kończąc rozważania w niniejszym rozdziale, analiza zawartych zagadnień nie wyczerpuje całej problematyki beneficjentów rzeczywistych. Nie ulega wątpliwości, że instytucja beneficjenta rzeczywistego w państwach Unii Europejskiej jest powszechnie uważana za jedno z najbardziej skomplikowanych zagadnień dotyczących stosowania przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[48].

[48] A. Golonka, *Zakres podmiotowy ustawy z przeciwdziałaniu praniu pieniędzy w świetle znowelizowanych przepisów*, Uniwersytet im. Adama Mickiewicza w Poznaniu, Poznań 2020, s. 162.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Adam Krupa
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 4.

ANALIZA RYZYKA – PROBLEMATYKA OUTSOURCINGU PROCESÓW ZWIĄZANYCH Z AML/CFT

4.1. UWAGI WPROWADZAJĄCE

Outsourcing definiowany jest zwykle jako przedsięwzięcie polegające na wydzieleniu ze struktury organizacyjnej przedsiębiorstwa macierzystego realizowanych przez nie funkcji i przekazaniu ich do realizacji innym podmiotom gospodarczym[1]. Specjaliści zajmujący się problematyką outsourcingu na gruncie polskim traktują tę koncepcję najczęściej jako formę restrukturyzacji[2]. Outsourcing to również „możliwość korzystania z kompleksowych usług, jakie oferują zewnętrzni wykonawcy (oferenci). Celowość korzystania z outsourcingu wymaga nie tylko wybrania właściwego oferenta, ale także dokładnego określenia potrzeb na usługi, które mogą być zaspokojone przez wykonawców zewnętrznych, i rzetelnej kalkulacji ich opłacalności (cena zakupu, jakość, rzetelność wykonawstwa)"[3].

Wyrazem przyjętej filozofii działania w tym zakresie pozostaje słynna sentencja sformułowana w 1923 r. przez H. Forda, sławnego potentata przemysłu samochodowego, która w dzisiejszych czasach jest uważana za podstawową zasadę outsourcingu: „Jeśli jest coś, czego nie potrafimy zrobić wydajniej, taniej i lepiej niż nasi

[1] M. Trocki, *Outsourcing*, PWE, Warszawa 2001, s. 13.
[2] A. Nalepka, *Restrukturyzacja przedsiębiorstw*, PWN, Warszawa–Kraków 1999.
[3] J. Penc, *Leksykon biznesu*, Placet, Warszawa 1997, s. 302.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

konkurenci, nie ma sensu, żebyśmy to robili. Powinniśmy zatrudnić do wykonania tej pracy kogoś, kto zrobi to lepiej"[4].

Powszechnie uważa się, że koncepcja outsourcingu jest wynalazkiem XX wieku, jednak elementy outsourcingu pojawiły się już znacznie wcześniej. Za pierwszą z jego form uznaje się powierzanie zakonom organizacji struktur edukacyjnych przez władców państw europejskich czy zlecanie przez Napoleona firmom prywatnym dostaw amunicji na pola bitew oraz zbierania rannych[5]. Gwałtowny wzrost zainteresowania outsourcingiem notuje się na 2004 r., kiedy to zaczęto wskazywać na poważną rolę w gospodarce światowej zjawiska przenoszenia działalności przedsiębiorstw za granicę (*offshore outsourcing* lub *offshoring*) i publicznie analizować wpływ stosowania tej strategii w krajach rozwiniętych na wzrost bezrobocia i stagnację gospodarczą[6].

Samo wyrażenie „outsourcing" stanowiące połączenie angielskich słów: *outside* (na zewnątrz) *resource* (zasób, źródło, pomoc naukowa) *using* (używanie, stosowanie, korzystanie) zostało po raz pierwszy użyte w 1979 r. i odnosiło się do kupowania niemieckich projektów przez brytyjski przemysł motoryzacyjny[7].

W ujęciu ogólnym outsourcing jest metodą (koncepcją) zarządzania, która sprowadza się do zawężenia zakresu zadań realizowanych bezpośrednio przez dane przedsiębiorstwo (określane jako firma macierzysta) i powierzenia ich do stałej realizacji przez inne podmioty gospodarcze (określane jako firmy usługowe). Idea outsourcingu zakłada, że dla prawie każdej funkcji, obszaru, procesu, które mogłyby być realizowane w ramach klasycznej struktury organizacyjnej przedsiębiorstwa można znaleźć alternatywę w postaci usług oferowanych przez zewnętrznych, wyspecjalizowanych dostawców (partnerów). Z tego powodu outsourcing określany jest jako metoda stałej obsługi zewnętrznej przez wyspecjalizowane podmioty, zarządzanie zewnętrzne, eksternalizacja czy wręcz dezintegracja działalności przedsiębiorstwa[8].

Przyjmuje się, że najważniejszymi powodami stosowania outsourcingu przez przedsiębiorstwa są[9]:

[4] W.M. Grudzewski, I.K. Hejduk, *Projektowanie systemów zarządzania*, Difin, Warszawa 2004, s. 210

[5] Angelika Wodecka-Hyjek, Zeszyty Naukowe nr 775 Uniwersytetu Ekonomicznego w Krakowie, Kraków 2008, s. 97.

[6] J. Bhagwati, A. Panagariya, T.N. Srinivsan, *The Muddles over Outsourcing*, „Journal of Economic Perspectives", vol. 18 (4). s. 93.

[7] M. Amiti, W. Shang-Jin., *Fear of Service Outsourcing. Is It Justified?*. „IMF Working Paper" 2004, s. 6–7.

[8] M. Matejun, *Outsourcing* (w:) *Kompendium metod i technik zarządzania. Teoria i ćwiczenia*, red. Szymańska, Oficyna a Wolters Kluwer business, Warszawa 2015, s. 211.

[9] Ch.L. Gay, *Outsourcing strategiczny: koncepcja, modele i wdrażanie*, Oficyna Ekonomiczna, Kraków 2002.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- obniżenie i bardziej efektywna kontrola kosztów operacyjnych,
- możliwość koncentrowania się na kluczowych kompetencjach przedsiębiorstwa, będących podstawą jego przewagi konkurencyjnej,
- pozyskanie zasobów, którymi przedsiębiorstwo nie dysponuje, w tym wiedzy eksperckiej i know-how partnerów,
- przyspieszenie pojawienia się korzyści z restrukturyzacji,
- pozyskanie kapitału,
- podział ryzyka,
- zwiększenie elastyczności działania poprzez możliwość szybkiego dostosowania skali działalności do zapotrzebowania na czynniki produkcji (tzw. skalowalność, ang. *scalability*)[10].

Badania przeprowadzone w 2002 r. przez portal Information Week na próbie 700 przedsiębiorstw ze Stanów Zjednoczonych wskazały, że ponad 60% respondentów wskazało oszczędności jako podstawowy cel zastosowania outsourcingu. Ponad połowa ankietowanych wymieniła również kwestie specjalizacji operacyjnej i sprawy pracownicze[11].

4.2. CHARAKTER PRAWNY UMOWY DOTYCZĄCEJ OUTSOURCINGU

Ze względu na kluczowe zagadnienie poruszane w niniejszym opracowaniu, którym są procedury bezpieczeństwa finansowego, przyjąć należy, że outsourcingiem będzie nabywanie przez instytucje obowiązane od podmiotu trzeciego szeroko pojętych usług wspierających stosowanie środków bezpieczeństwa finansowego określonych w ustawie o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu[12].

W odróżnieniu od wielu ustawodawstw europejskich w polskim kodeksie cywilnym umowy o świadczenie usług nie zostały odrębnie uregulowane. Ustawodawca w art. 750 Kodeksu cywilnego posłużył się techniką odesłania do przepisów o zleceniu (art. 734–749 i 751 pkt 1) w odniesieniu do tych umów o świadczenie usług[13], które nie zostały uregulowane innymi przepisami. Świadczenie usług występuje w przypadku wszelkich umów obligujących do dokonywania czyn-

[10] A. Grycuk, *Klastry a rozwój regionalny. Klaster usług biznesowych w Krakowie*, „Studia BAS" 2017, vol. 1 (49), s. 144.

[11] R. Gareiss, *Analysing the Outsourcers*, 18 listopada 2002 (data dostępu: 13 maja 2010).

[12] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2021 r., poz. 1132).

[13] P. Gołębiewski, *Wpływ AML na sektor usług rachunkowych*, Kortowski Przegląd Prawniczy Uniwersytetu Warmińsko-Mazurskiego w Olsztynie, Olsztyn 2019, s. 50–79.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ności faktycznych (jednorazowych, wielokrotnych, w tym wykonywanych stale) lub do dokonania powiązanych funkcjonalnie czynności faktycznych i prawnych (np. umowy o świadczenie pomocy prawnej, zarządzanie przedsiębiorstwem, majątkiem lub nieruchomością). Wskazać należy na dwie podstawowe cechy charakterystyczne dla tych umów: świadczenie główne dłużnika polega na czynieniu, a nie na daniu, a odpowiedzialność odszkodowawcza powstaje w razie niedołożenia należytej staranności (art. 355 k.c.) i nie jest uzależniona od uzyskania przez dłużnika oznaczonego rezultatu. Umowy o świadczenie usług należą do tzw. obrotu uniwersalnego, a ich stronami mogą być zarówno przedsiębiorcy, jak i konsumenci.

Zlecenie, a zatem i umowa o świadczenie usług, jest umową konsensualną i dwustronnie zobowiązującą. Może być ona odpłatna lub nieodpłatna. Umowa zlecenia nie wymaga zachowania formy szczególnej. Zasada ta pozostaje aktualna niezależnie od tego, co jest przedmiotem zleconej czynności.

Ustawa nie stawia ograniczeń podmiotowych. Zarówno dającym zlecenie, jak też przyjmującym zlecenie, mogą być wszelkie podmioty prawa cywilnego, jednakże wymóg określonych kwalifikacji podmiotowych, szczególnie przyjmującego zlecenie, może wynikać z charakteru zlecenia. Ma to miejsce przy np. zleceniu na dokonywanie czynności prawnych zastrzeżonych dla adwokatów lub radców prawnych[14].

Stosując odpowiednio przepisy o zleceniu, należy przede wszystkim uwzględniać istotę stosunku prawnego wynikającego z nienazwanej umowy o świadczenie usług i ewentualne różnice pomiędzy istotnymi elementami tego stosunku a elementami ukształtowanego w kodeksie typu umowy zlecenia[15]. Stosowanie odpowiednie przepisów o zleceniu oznacza konieczność uwzględnienia specyfiki konkretnej sytuacji[16].

4.3. RAMY PRAWNE OUTSOURCINGU W SYSTEMIE BEZPIECZEŃSTWA FINANSOWEGO

Tak jak w innych branżach oraz sferze współpracy pomiędzy niezależnymi podmiotami, outsourcing również w zakresie powierzania stosowania środków bezpieczeństwa finansowego najczęściej będzie oparty o postanowienia umowy o świadczeniu usług, do której zastosowanie mają przede wszystkim przepisy o zleceniu[17].

[14] R. Morek (w:) *Kodeks cywilny*.., t. 3b, red. K. Osajda, 2017, kom. do art. 734, nt 1.

[15] Tak w wyroku SN z dnia 20 lipca 2006 r., V CSK 115/06, LEX nr 1044085.

[16] Tak w wyroku SN z dnia 23 stycznia 2008 r., V CSK 377/07.

[17] P. Sitek, *Rosnąca rola banków w kreacji pieniądza* (w:) *Pieniądz i jego oddziaływanie na otoczenie*, Wyższa Szkoła Finansów i Zarządzania w Warszawie, Warszawa 2016.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

W omawianej kwestii, jako *lex specialis* wobec przepisów Kodeksu cywilnego należy traktować przede wszystkim przepisy ustawy o przeciwdziałaniu praniu pieniędzy i finansowania terroryzmu, które wyznaczają ramy współpracy instytucji obowiązanych z podmiotami trzecimi w zakresie stosowania środków bezpieczeństwa finansowego.

Przed omówieniem tych przepisów w pierwszej kolejności należy wskazać czym są środki bezpieczeństwa finansowego. Są to czynności i działania będące elementem systemu bezpieczeństwa finansowego, określone w ustawie, do których podejmowania zobowiązane są instytucje obowiązane. Obejmują one identyfikację klienta oraz weryfikację jego tożsamości; identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli – w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej. Obejmują też ocenę stosunków gospodarczych i, stosownie do sytuacji, uzyskanie informacji na temat ich celu i zamierzonego charakteru; bieżące monitorowanie stosunków gospodarczych klienta, w tym analizę transakcji przeprowadzanych w ramach stosunków gospodarczych w celu zapewnienia, że transakcje te są zgodne z wiedzą instytucji obowiązanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz zgodne z ryzykiem prania pieniędzy oraz finansowania terroryzmu związanym z tym klientem, jak również badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta – w przypadkach uzasadnionych okolicznościami, zapewnienie, że posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych są na bieżąco aktualizowane.

Zgodnie z ustawą instytucje obowiązane dokumentują zastosowane środki bezpieczeństwa finansowego oraz wyniki bieżącej analizy przeprowadzanych transakcji. Na żądanie organów bezpieczeństwa finansowego instytucje obowiązane wykazują, że przy uwzględnieniu poziomu rozpoznanego ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z danymi stosunkami gospodarczymi lub transakcją okazjonalną zastosowały odpowiednie środki bezpieczeństwa finansowego.

Instytucje obowiązane na potrzeby stosowania środków bezpieczeństwa finansowego mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie. Przed nawiązaniem stosunków gospodarczych lub przeprowadzeniem transakcji okazjonalnej instytucje obowiązane informują klienta o przetwarzaniu jego danych osobowych, w szczególności o obowiązkach instytucji obowiązanej wynikających z ustawy w zakresie przetwarzania tych danych.

Zgodnie z art. 47 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu instytucje obowiązane mogą korzystać z usług podmiotu trzeciego przy stosowaniu środków bezpieczeństwa finansowego, które obejmują identyfikację klienta oraz weryfikację jego tożsamości; identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu:

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- weryfikacji jego tożsamości,
- ustalenia struktury własności i kontroli – w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej,
- oceny stosunków gospodarczych i, stosownie do sytuacji, uzyskanie informacji na temat ich celu i zamierzonego charakteru.

Warunkiem dopuszczającym świadczenie tych usług jest to, aby podmiot trzeci co do zasady nie miał siedziby w państwie trzecim wysokiego ryzyka i aby niezwłocznie przekazywał, na żądanie instytucji obowiązanej, niezbędne informacje oraz dokumenty dotyczące zastosowanych środków bezpieczeństwa finansowego, w tym kopie dokumentów uzyskanych podczas stosowania środków bezpieczeństwa finansowego polegających na identyfikacji klienta i beneficjenta rzeczywistego oraz weryfikacji ich tożsamości.

Korzystanie z usług podmiotu trzeciego nie zwalnia instytucji obowiązanej z odpowiedzialności za zastosowanie środków bezpieczeństwa finansowego.

Podmiotem trzecim, o którym mowa w ust. 1, może być instytucja obowiązana lub podmiot z siedzibą w innym państwie lub organizacja członkowska lub federacja zrzeszająca taki podmiot, który na podstawie właściwych przepisów tego państwa z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu jest obowiązany do stosowania środków bezpieczeństwa finansowego i przechowywania dokumentów i informacji oraz podlega nadzorowi właściwych organów tego państwa w sposób odpowiadający wymogom wynikającym z przepisów Unii Europejskiej z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

Analiza przywołanej regulacji wskazuje, że instytucja obowiązana stosując wybrane środki bezpieczeństwa finansowego może posiłkować się wsparciem podmiotów trzecich. Należy jednak zauważyć, że w tym wypadku instytucja obowiązana stosuje środki bezpieczeństwa finansowego samodzielnie. Wsparcie podmiotu trzeciego może dotyczyć wyłącznie podstawowych obowiązków tej instytucji. Ustawodawca nie wskazał wprost, na czym konkretnie może polegać współpraca podmiotów, jednak zauważyć trzeba, że omawiany przepis daje możliwość podjęcia współpracy pomiędzy instytucjami obowiązanymi, które mogą wzajemnie przekazywać sobie informacje oraz dokumenty dotyczące zastosowanych środków bezpieczeństwa finansowego, w tym kopie dokumentów uzyskanych podczas stosowania środków bezpieczeństwa finansowego polegających na identyfikacji klienta i beneficjenta rzeczywistego oraz weryfikacji ich tożsamości.

Jednocześnie ustawodawca nie wskazał, czy taka współpraca instytucji obowiązanej z podmiotem trzecim ma mieć charakter odpłatny, jednak wydaje się, że nie ma ku temu przeszkód. W takim przypadku współpraca w pewnych przypadkach mogłaby wypełniać definicję outsourcingu.

Zgodnie z art. 48 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu instytucje obowiązane mogą powierzyć stosowanie środków bezpie-

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

czeństwa finansowego[18] oraz prowadzenie i dokumentowanie wyników bieżącej analizy przeprowadzanych transakcji osobie fizycznej, osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej działającej w imieniu i na rzecz instytucji obowiązanej, jeżeli na podstawie pisemnej umowy podmiot, któremu powierzono stosowanie środków bezpieczeństwa finansowego, ma być traktowany jako część instytucji obowiązanej. Powierzenie stosowania środków bezpieczeństwa finansowego nie zwalnia jednak instytucji obowiązanej z odpowiedzialności za zastosowanie środków bezpieczeństwa finansowego.

Oznacza to, że instytucje obowiązane mogą korzystać ze wsparcia wyspecjalizowanych podmiotów w zakresie procesów związanych z obowiązkami systemu bezpieczeństwa finansowego[19], jednakże w takiej sytuacji nadal instytucja obowiązana ponosi pełną odpowiedzialność za prawidłowe stosowanie środków bezpieczeństwa finansowego.

4.4. OUTSOURCING PROCESÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM FINANSOWYM W WYBRANYCH INSTYTUCJACH OBOWIĄZANYCH

Ustawa dając możliwość powierzenia przez instytucję obowiązaną stosowania środków bezpieczeństwa finansowego nie przewiduje w tym względzie wyłączeń podmiotowych lub przedmiotowych. Jednak instytucje obowiązane, wskazane w art. 2 ustawy, przy powierzeniu stosowania środków bezpieczeństwa finansowego oraz prowadzenia i dokumentowania wyników bieżącej analizy przeprowadzanych transakcji powinny stosować przepisy omawianej ustawy, przepisy prawa, które dotyczą danej grupy instytucji obowiązanych, oraz takie, które odnoszą się do wszystkich uczestników obrotu.

Do tej ostatniej kategorii przepisów należą z pewnością przepisy z zakresu ochrony danych osobowych[20], które mają zastosowanie, w przypadku gdy niezależne podmioty przekazują dane osobowe osób fizycznych. Biorąc pod uwagę, że procesy związane z bezpieczeństwem finansowym wymagają przetwarzania

[18] P. Sitek, *Wybrane aspekty kryzysów finansowych* (w:) *Prawo bezpieczeństwa finansowego*, Wydział Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego, Olsztyn 2016.

[19] P. Gołębiewski, *System przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w Polsce* (w:) *Wyzwania i szanse dla polskiego sektora bankowego*, red. P. Sitek, recenzowana praca zbiorowa, Wyższa Szkoła Finansów i Zarządzania w Warszawie, Warszawa 2016, s. 97–126.

[20] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4 maja 2016 r.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

takich danych osobowych, jak nazwisko, numer PESEL osób czy adres zamieszkania należy przyjąć, że umowa zawarta pomiędzy instytucją obowiązaną a niezależnym podmiotem, któremu powierzono stosowanie środków bezpieczeństwa finansowego powinna uwzględniać zasady określone w oparciu o treść art. 6 ust. 1 lit. a, b, c. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE w związku chociażby z art. 28 RODO.

Obecnie zarówno w dziedzinie RODO, jak i bezpieczeństwa finansowego dominuje podejście oparte na ryzyku, co oznacza, że obie regulacje nie wskazują gotowych rozwiązań, które są identyczne dla wszystkich podmiotów. Prezentują natomiast potencjalne obszary związane z zagrożeniami oraz listę działań mających na celu przeciwdziałanie praniu pieniędzy, finansowaniu terroryzmu i naruszeniom w obszarze danych osobowych.

Zgodnie z tym podejściem, każda instytucja obowiązana może dostosować procedury i środki bezpieczeństwa do swojej indywidualnej sytuacji, branży, wielkości firmy, zasięgu geograficznego, skali i rodzaju prowadzonej działalności. Rodzi to jednak ryzyko popełnienia błędów w realizacji obowiązków ustawowych ze względu na ograniczoną wiedzę czy niewystarczające zasoby (m.in. zaangażowanie w inne obowiązki oraz niedobór pracowników) danego podmiotu. Dlatego w tym zakresie doradztwo o charakterze eksperckim może być ważnym elementem zapewnienia prawidłowości realizacji środków bezpieczeństwa finansowego przez instytucje obowiązane.

Określona w ustawie możliwość outsourcingu zadań związanych ze stosowaniem środków bezpieczeństwa finansowego powinna uwzględniać również przepisy dotyczące poszczególnych grup instytucji obowiązanych. Przykładem mogą być tutaj ustawy dotyczące radców prawnych[21], adwokatów[22], notariuszy[23] lub doradców podatkowych[24] w zakresie chociażby realizacji obowiązku zachowania w tajemnicy faktów i informacji, które dana instytucja obowiązana uzyskała w związku ze świadczoną pomocą z zakresu poszczególnych profesji. Analizując przepisy regulujące obowiązek zachowania tajemnicy przez przedstawicieli poszczególnych zawodów prawniczych zwrócić należy uwagę, że nie dotyczy on informacji udostępnianych na podstawie przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w zakresie określonym tymi przepisami. Jednak chociaż przepisy dotyczące powierzenia stosowania środków bezpieczeństwa finansowego innemu podmiotowi działającemu w imieniu i na rzecz instytucji obowiązanej są częścią ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,

[21] Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (Dz.U. z 2020 r., poz. 75).

[22] Ustawa z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz.U. z 2020 r., poz. 1651).

[23] Ustawa z dnia z dnia 14 lutego 1991 r. Prawo o notariacie (Dz.U. z 2020 r., poz. 1192).

[24] Ustawa z dnia 5 lipca 1996 r. o doradztwie podatkowym (Dz.U. z 2020 r., poz. 130).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

to należy przyjąć, że wyłączenie obowiązku zachowania tajemnicy dotyczy przekazywania informacji organom informacji finansowej, a nie podmiotowi, któremu instytucja obowiązana miałby powierzyć stosowanie środków bezpieczeństwa. Może być to istotną przeszkodą dla podjęcia przez tę grupę instytucji obowiązanych współpracy z podmiotami, które miałby w imieniu i na rzecz tej instytucji stosować środki bezpieczeństwa finansowego. Jednocześnie w ustawach dotyczących zawodów prawniczych brak jest wyczerpującego określenia zasad współpracy z podmiotami zewnętrznymi oraz jednoznacznych wytycznych w zakresie udostępniania tym podmiotom informacji objętych tajemnicą zawodową.

Koleją ważną grupę instytucji obowiązanych stanowią zakłady ubezpieczeń wykonujące działalność, o której mowa w dziale I załącznika do ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2020 r., poz. 895, 1180 i 2320 oraz z 2021 r., poz. 355 i 680), w tym krajowe zakłady ubezpieczeń, główne oddziały zagranicznych zakładów ubezpieczeń z siedzibą w państwie niebędącym państwem członkowskim oraz oddziały zagranicznych zakładów ubezpieczeń mających siedzibę w innym niż Rzeczpospolita Polska państwie członkowskim Unii Europejskiej.

Ta grupa instytucji obowiązanych stosuje wobec osób uprawnionych z tytułu umów ubezpieczenia środki bezpieczeństwa finansowego, o których mowa w art. 34 ust. 1 pkt 1. ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Środki te są stosowane niezwłocznie po ustaleniu osób uprawnionych z tytułu umowy ubezpieczenia, nie później niż w momencie wypłaty świadczenia. W przypadku uzyskania informacji o częściowym lub całkowitym przeniesieniu praw z tytułu umowy ubezpieczenia instytucje te stosują wobec osób uprawnionych z tytułu tych umów środek bezpieczeństwa finansowego, polegający na identyfikacji beneficjenta rzeczywistego oraz podejmowaniu uzasadnionych czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli – w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej.

Ustawa regulująca funkcjonowanie tych podmiotów[25] definiuje outsourcing jako umowę między zakładem ubezpieczeń albo zakładem reasekuracji a dostawcą usług, na podstawie której dostawca usług wykonuje proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez zakład ubezpieczeń lub zakład reasekuracji, a także umowę, na podstawie której dostawca usług powierza wykonanie takiego procesu, usługi lub działania innym podmiotom, za pośrednictwem których wykonuje on dany proces, usługę lub działanie[26].

[25] Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r., poz. 1130).

[26] Art. 3 ust. 1 pkt 27 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r., poz. 1130).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Zakład ubezpieczeń i osoby w nim zatrudnione, a także osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia. Obowiązek zachowania tajemnicy nie dotyczy jednak informacji udzielanych między innymi na wniosek zleceniobiorców czynności ubezpieczeniowych i reasekuracyjnych oraz funkcji należących do systemu zarządzania powierzanych w drodze outsourcingu w zakresie, w jakim dotyczą one zleconych czynności i funkcji[27].

Funkcją należącą do systemu zarządzania jest zdolność zakładu ubezpieczeń lub zakładu reasekuracji do wykonywania poszczególnych zadań w ramach systemu zarządzania[28], a zatem będzie nią funkcja zgodności z przepisami i funkcja audytu wewnętrznego[29]. Biorąc to pod uwagę należy dojść do wniosku, że stosowanie przez zakład ubezpieczeń lub zakład reasekuracji środków bezpieczeństwa finansowego jest zadaniem wykonywanym w ramach systemu zarządzania.

Powierzenie stosowania środków bezpieczeństwa finansowego jest w przypadku omawianej grupy instytucji obowiązanych prawnie dopuszczalne[30], jednak jest uzależnione od podjęcia wielu działań określonych w ustawie. W pierwszej kolejności zakład ubezpieczeń lub zakład reasekuracji zobowiązany jest do przygotowania na piśmie zasad zarządzania ryzykiem[31], a następnie informują organ nadzoru o zamiarze wprowadzenia tych zasad oraz o ich istotnej zmianie. Dostawca usług musi przede wszystkim współpracować z organem nadzoru i poddawać się jego kontroli oraz mieć dostęp do danych związanych ze świadczoną usługą. Outsourcing funkcji należących do systemu zarządzania oraz podstawowych lub ważnych czynności nie może odbywać się w sposób prowadzący do przekazania zarządzania zakładem ubezpieczeń lub zakładem reasekuracji, o którym mowa w art. 368 § 1 ustawy z dnia 15 września 2000 r. – Kodeks spółek handlowych; przekazania wykonywania działalności ubezpieczeniowej lub reasekuracyjnej w sposób powodujący brak faktycznego wykonywania działalności przez zakład ubezpieczeń lub zakład reasekuracji; pogorszenia jakości systemu zarządzania zakładu ubezpieczeń lub zakładu reasekuracji; zwiększenia ryzyka operacyjnego zakładu ubezpieczeń lub zakładu reasekuracji; pogorszenia możliwości monitorowania przez organ nadzoru przestrzegania przez zakład ubezpieczeń lub zakład

[27] Art. 35 ust. 2 pkt 1 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r., poz. 1130).

[28] Art. 3 ust. 1 pkt 1 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r., poz. 1130).

[29] Art. 3 ust. 1 pkt 46 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r., poz. 1130).

[30] Art. 73 ust. 3 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r., poz. 1130).

[31] Art. 46 ust. 1 pkt 4 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r., poz. 1130).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

reasekuracji jego obowiązków; pogorszenia jakości świadczenia usług ubezpieczającym, ubezpieczonym lub uprawnionym z umów ubezpieczenia oraz cedentom.

Podkreślenia wymaga to, że organ nadzoru zakładu ubezpieczeń lub zakładu reasekuracji może, w drodze decyzji, zakazać planowanego outsourcingu funkcji należących do systemu zarządzania oraz podstawowych lub ważnych czynności, a także istotnej zmiany takiej umowy outsourcingu, w przypadku stwierdzenia, że wykonywanie tych funkcji i czynności mogłoby odbywać się z naruszeniem warunków, o których mowa w art. 73–77 ustawy o działalności ubezpieczeniowej i reasekuracyjnej. Organ nadzoru może, w drodze decyzji, nakazać zakładowi ubezpieczeń i zakładowi reasekuracji rozwiązanie w wyznaczonym terminie umowy outsourcingu w przypadku stwierdzenia, że wykonywanie funkcji należących do systemu zarządzania oraz podstawowych lub ważnych czynności odbywa się z naruszeniem warunków.

Jednym z najważniejszych elementów systemu zapobiegania praniu pieniędzy oraz finansowania terroryzmu są banki[32]. W tym wypadku w kwestii powierzenia podmiotowi zewnętrznemu jakichkolwiek czynności jedną z wiodących ról pełni zabezpieczenie przed ujawnieniem tajemnicy bankowej. Bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje[33].

Umowa, w ramach której zostaje powierzone wykonywanie czynności, powinna zawierać zobowiązanie, że dostawca usług zapewni ochronę informacji poufnych, osobowych lub innych informacji szczególnie chronionych i spełnia wszystkie wymogi prawne dotyczące ochrony danych, które mają zastosowanie do banków (np. ochrona danych osobowych, oraz w stosownych przypadkach przestrzeganie obowiązku zachowania tajemnicy bankowej lub podobnych obowiązków w zakresie poufności w odniesieniu do informacji klientów)[34].

Ramy prawne outsourcingu dopuszczalnego w działalności bankowej zawarte są w pierwszej kolejności w Prawie bankowym oraz subsydiarnie w Wytycznych EBA[35]. Prawo bankowe nie zawiera definicji pojęcia outsourcingu, jednakże należy przyjąć, że pojęcie outsourcingu w rozumieniu Wytycznych EBA[36] obejmuje powierzenie przedsiębiorcy wykonywania w imieniu banku pośrednictwa

[32] *Prawo bezpieczeństwa finansowego*, red. P. Sitek, M. Karpiuk, M. Sawicka, Wydział Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego, Olsztyn 2016, s. 339.

[33] Art. 104 ust. 1 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. z 2020 r., poz. 1896).

[34] Stanowisko UKNF dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnieniem w działalności banków, Warszawa, 16 września 2019, s. 11.

[35] Wytyczne w sprawie outsourcingu z dnia 25 lutego 2019 r. Europejski Urząd Nadzoru Bankowego EBA/GL/2019/02.

[36] EBA – Europejski Urząd Nadzoru Bankowego.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

w zakresie czynności, o których mowa w art. 5 oraz 6 Prawa bankowego, szczegółowo opisanych w art. 6a ust. 1 pkt 1–2[37].

Z uwagi na definicję „outsourcingu" zawartą w Wytycznych EBA, zgodnie z którą outsourcing oznacza umowę w dowolnej formie zawartą między instytucją, instytucją płatniczą lub instytucją pieniądza elektronicznego a usługodawcą, na mocy której usługodawca realizuje proces, usługę lub zadanie, które w przeciwnym razie byłoby realizowane przez samą instytucję, instytucję płatniczą lub instytucję pieniądza elektronicznego, należy przyjąć iż „outsourcing" jest pojęciem szerszym niż powierzenie wykonywania czynności w rozumieniu Prawa bankowego. Mając to na uwadze za „powierzenie wykonywania czynności" należy uznać powierzenie wykonywania czynności w reżimie art. 6a i następnych Prawa bankowego. Natomiast ilekroć używane jest pojęcie „outsourcingu", należy przyjąć, że mowa jest o tej kategorii w rozumieniu Wytycznych EBA, zatem, obejmującej także powierzanie wykonywania czynności. Pojęcie „powierzenia wykonywania czynności", o którym mowa w art. 6a Prawa bankowego mieści się w pojęciu powierzenia „funkcji" z Wytycznych EBA.

Należy zatem w outsourcingu dopuszczonym przez Prawo bankowe oraz Wytyczne EBA wyróżnić pośrednictwo w zakresie czynności bankowych, które zostało określone w art. 6a ust. 1 pkt 1 oraz powierzenie wykonywania czynności, określone w art. 6a ust. 1 pkt 2 tej ustawy.

Pośrednictwo w zakresie czynności bankowych to stosunek prawny, na podstawie którego bank w drodze umowy zawartej na piśmie powierza przedsiębiorcy lub przedsiębiorcy zagranicznemu wykonywanie w imieniu i na rzecz banku pośrednictwa w zakresie czynności bankowych, polegającego na zawieraniu i zmianie umów rachunków bankowych, zawieraniu i zmianie określonych umów kredytów i pożyczek pieniężnych, ugód, ustanawianiu zabezpieczeń, zawieranie umów o kartę płatniczą, przyjmowaniu wpłat, dokonywaniu wypłat oraz obsłudze czeków związanych z prowadzeniem rachunków bankowych przez ten bank, dokonywaniu wypłat i przyjmowaniu spłat udzielonych przez ten bank kredytów i pożyczek pieniężnych, przyjmowaniu wpłat na rachunki bankowe prowadzone przez inne banki oraz dyspozycji przeprowadzania bankowych rozliczeń pieniężnych związanych z prowadzeniem rachunków bankowych przez ten bank, wykonywaniu czynności związanych z emitowaniem i przechowywaniem bankowych papierów wartościowych oraz innych papierów wartościowych, a także wykonywaniu innych czynności zleconych związanych z emisją i obsługą papierów wartościowych, windykacji należności banku, wykonywaniu innych czynności, po uzyskaniu zezwolenia Komisji Nadzoru Finansowego[38].

[37] Stanowisko UKNF dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnieniem w działalności banków, Warszawa, 16 września 2019, s. 12.

[38] Art. 6a ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U z 2020 r., poz. 1896).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Pośrednictwem w zakresie czynności bankowych będzie zatem powierzenie czynności, które stanowią istotę odpłatnej działalności banku jako przedsiębiorcy, który udostępnia środki pieniężne, przyjmuje je jako depozyty i udostępnia efektywne narzędzia obrotu pieniężnego. Powierzenie większości z wyżej wskazanych czynności następuje na podstawie umowy agencyjnej.

Druga grupą czynności, które mogą stanowić przedmiot outsourcingu, są czynności faktyczne związane z działalnością bankową. Prawo bankowe w art. 6a ust. 1 pkt 2) stanowi, że bank może w drodze umowy zawartej na piśmie powierzyć przedsiębiorcy wykonywanie czynności faktycznych związanych z działalnością bankową. Muszą być one bezpośrednio związane z działalnością bankową, tzn. stanowić czynności cząstkowe (składowe) czynności wymienionych w art. 5 i 6 Prawa bankowego lub tych, bez których podjęcia nie byłoby możliwe należyte wykonanie określonej umowy. Powierzenie wykonywania tych czynności w ramach outsourcingu jest dopuszczalne i nie wymaga uzyskania zezwolenia KNF[39]. Dla przesądzenia, czy dana czynności objęta jest tym pojęciem, istotny jest związek tej czynności z działalnością bankową, a dokładniej stwierdzenie, czy dana czynność jest bezpośrednio związana z działalnością bankową. Wyłącznie bezpośredni związek z czynnościami, o których mowa w art. 5 ust. 1 i 2 oraz 6 ust. 1 prawa bankowego, pozwala zakwalifikować daną usługę do kategorii, o której mowa w art. 6a ust. 1 pkt 2[40]. Przykładem takiej czynności może być wykorzystanie zasobów teleinformatycznych podmiotów trzecich w ramach chmury obliczeniowej do działalności bankowej, jednak wówczas na banku spoczywa obowiązek wykazania istnienia związku z działalnością bankową. Związek ten powinien mieć charakter funkcjonalny i nie jest wystarczające wykazanie przez bank jedynie korzyści wynikających ze stosowania skalowalnych zasobów w ramach usługi świadczonej w chmurze obliczeniowej[41].

Należy zauważyć, że zarówno powierzenie wykonywania czynności pośrednictwa w zakresie czynności bankowych, jak i powierzenie wykonywania czynności faktycznych nie może obejmować zarządzania bankiem w rozumieniu art. 368 § 1 ustawy z dnia 15 września 2000 r. – Kodeks spółek handlowych (Dz.U. z 2020 r., poz. 1526), zwanej dalej „Kodeksem spółek handlowych", oraz w rozumieniu art. 48 ustawy z dnia 16 września 1982 r. – Prawo spółdzielcze (Dz.U. z 2020 r., poz. 275, 568, 695 i 875), zwanej dalej „ustawą – Prawo spółdzielcze", w szczególności zarządzania ryzykiem związanym z prowadzeniem działalności bankowej, w tym zarządzania aktywami i pasywami, dokonywania oceny zdol-

[39] Stanowisko UKNF dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnieniem w działalności banków, Warszawa, 16 września 2019, s. 4.

[40] A. Żygadło, *Usługa cloud computingu jako czynność faktyczna związana z działalnością bankową*, „Monitor Prawa Bankowego "2013, nr 7–8, s. 83–94.

[41] A. Krasuski, *Korzystanie z chmury obliczeniowej przez instytucje w świetle RODO*, „Monitor Prawa Bankowego" 2019, nr 7–8, s. 60–73.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ności kredytowej i analizy ryzyka kredytowego, jak również przeprowadzania audytu wewnętrznego banku.

Zgodnie z art. 368 § 1 KSH zarząd prowadzi sprawy spółki i reprezentuje spółkę. Zgodnie z art. 48 Prawa spółdzielczego zarząd kieruje działalnością spółdzielni oraz reprezentuje ją na zewnątrz (§ 1). Podejmowanie decyzji niezastrzeżonych w ustawie lub statucie dla innych organów należy do zarządu (§ 2). Zarządzanie bankiem w rozumieniu art. 6a, ust. 3, pkt 1) Prawa bankowego obejmuje prowadzenie spraw (kierowanie) banku oraz jego reprezentację. Prowadzenie spraw (kierowanie) banku polega nie tylko na kierowaniu bieżącą działalnością banku (tj. nadzorowaniu i kontrolowaniu przebiegu działalności), lecz również zarządzaniu w szerokim znaczeniu tego słowa, tj. świadomym podejmowaniu decyzji mających za przedmiot rozstrzyganie spraw istotnych dla funkcjonowania banku i dokonywaniu wyboru celów, sposobów i środków działania, przejawiającym się w szczególności w:

- organizowaniu działalności – ustalaniu struktury organizacyjnej i sposobu, w jaki mają być wykonywane poszczególne operacje i inne czynności (procedury),
- wytyczaniu polityki, w tym globalnej strategii – ogólnych kierunków działania w średnim, kilkuletnim okresie, jak również polityki szczegółowej, obejmującej konkretne zadania mające prowadzić do głównego celu,
- analizowaniu uzyskiwanych wyników i wyciąganiu wniosków dla dalszej działalności.

Określając charakter prawny powierzenia stosowania środków bezpieczeństwa finansowego należy uznać, że nie będzie ono pośrednictwem w zakresie czynności bankowych. Ze względu jednak na charakter tych procesów należy uznać, że mają one funkcjonalny związek z czynnościami bankowymi i są elementem niezbędnym do ich przeprowadzenia. W związku z tym noszą one cechy czynności faktycznych określonych w art. 6a ust. 1 pkt 2 ustawy prawo bankowe. Istnieje pogląd jakoby stosowanie środków bezpieczeństwa finansowego przez podmiot zewnętrzny miało być realizowane na podstawie umowy agencyjnej, a więc być jedną z czynności pośrednictwa w zakresie czynności bankowych[42].

Bank zawierając zgodnie z art. 6a ust. 1 Prawa bankowego umowę, na podstawie której powierza dostawcy usługi wykonanie określonych w tym przepisie czynności, obowiązany jest w taki sposób określić w umowie swoje relacje z dostawcą usługi, aby nie doszło do przeniesienia kompetencji ustawowo przypisanych zarządowi banku[43]. Przyjmując, że kluczowe decyzje stanowiące elementy bankowych

[42] M.A. Kędzierski, „Prokuratura i Prawo" 2021, nr, 5, s. 89.

[43] Stanowisko UKNF dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnieniem w działalności banków, Warszawa, 16 września 2019, s. 6.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

procedur bezpieczeństwa finansowego wydają się pozostawać w domenie zarządzania bankiem w rozumieniu art. 368 § 1 ksh lub art. 48 ustawy Prawo spółdzielcze, należy dojść do wniosku, że nie wszystkie elementy systemu bezpieczeństwa finansowego mogą być przedmiotem powierzenia przez bank.

4.5. PODSUMOWANIE

Przyjmuje się, że zastosowanie outsourcingu bywa procesem trudnym i skomplikowanym. Według dostępnych badań[44] ponad 50% kontraktów outsourcingowych podlega renegocjowaniu, z czego 20% w trakcie pierwszych 12 miesięcy obowiązywania. Najczęściej spotykanymi problemami wiążącymi się z zastosowaniem outsourcingu w różnych dziedzinach są[45]:

- nieuzyskanie spodziewanych obniżek kosztów,
- ogólne pogorszenie jakości realizacji funkcji dotychczas wykonywanej samodzielnie,
- niepowodzenia w wypracowaniu relacji prawdziwej współpracy z dostawcą usług,
- spory między klientem a dostawcą usługi, zwłaszcza dotyczące jakości usługi i wysokości wynagrodzenia,
- niewykorzystanie szans z uzyskania większej operacyjnej elastyczności przy zaspokojeniu potrzeb klientów.

Inne wyróżniane niebezpieczeństwa wynikające ze stosowania outsourcingu to wystąpienie możliwości uzależnienia się od dostawcy, niemożność zachowania wysokiej jakości przy dużym udziale obcych komponentów, zatarcie obrazu firmy wśród klientów, możliwość poniesienia strat wynikających z niesolidności kooperantów, ujemne stosunki społeczne związane z redukcją personelu, ryzyko wzrostu kosztów.

Jako najczęstsze błędy popełniane przez kadrę kierowniczą przedsiębiorstw stosujących lub wdrażających outsourcing, mające wpływ na wystąpienie wskazanych problemów, wymieniane są[46]:

- niewłaściwy dobór kryteriów wyboru dostawcy,
- kierowanie się wyłącznie kryterium cenowym,
- słabe relacje nabywca–dostawca podczas życia projektu,
- niestosowanie charakterystyki świadczonych usług,
- nadmierna koncentracja na technologii i finansach,

[44] Gartner highlights outsourcing problems, 2005.

[45] Ch.L. Gay, *Outsourcing strategiczny: koncepcja, modele i wdrażanie*, Oficyna Ekonomiczna, Kraków 2002.

[46] W. Rogowski, *Błędna „5" outsourcingu*, „CIO Magazyn Dyrektorów IT" 2006.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- pomijanie aspektu personalnego,
- zbyt pośpiesznie przygotowywany kontrakt.

Wskazane powyżej zagrożenia mogą dotyczyć również powierzenia stosowania środków bezpieczeństwa finansowego. Specyficzne zagrożenia, z którymi mogą się spotkać instytucje obowiązane, wynikają w znacznej mierze z szerokiego zastosowanego przez ustawodawcę podejścia opartego na ryzyku, którego istotą jest założenie, że każdy z podmiotów zobowiązany do stosowania przepisów musi zidentyfikować potencjalne obszary, w których istnieje większe lub mniejsze zagrożenie prania pieniędzy, finansowania terroryzmu, naruszenia przetwarzania danych osobowych lub obowiązku zachowania tajemnicy.

Przejawem tego jest z pewnością brak systemu oceny usług podmiotów, którym instytucje obowiązane mogłyby powierzyć stosowanie środków bezpieczeństwa finansowego. Nie istnieje system certyfikacji takich podmiotów, które mogłyby świadczyć usługi w omawianym zakresie oraz standaryzacji ich procedur, które stanowiłyby gwarancje rzetelności i bezpieczeństwa współpracy. W konsekwencji powierzając tę niezwykle ważną część działalności instytucja obowiązana powinna uczestniczyć w niemal każdym etapie procedury stosowania środków bezpieczeństwa finansowego, co znacznie obniża racjonalność stosowania tego rozwiązania.

Jak to stwierdzono powyżej, w umowach o świadczenie usług odpowiedzialność odszkodowawcza powstaje w razie niedołożenia należytej staranności. Z drugiej strony brakuje jednolitych standardów świadczenia usług w zakresie stosowania środków bezpieczeństwa finansowego, które mogłyby stanowić miernik należytej staranności. W tym stanie rzeczy określenie praw i obowiązków stron umowy, która będzie podstawą współpracy z podmiotem wspierającym instytucję obowiązaną, w każdym przypadku będzie obarczone pewnym ryzykiem niedostatecznego ich określenia. Biorąc pod uwagę skalę możliwych negatywnych konsekwencji dla instytucji obowiązanej oraz potencjalne zyski, które wynikają z zastosowania outsourcingu, należy przypuszczać, że tylko niektóre instytucje obowiązane zdecydują się na zastosowanie tego modelu operacyjnego. Wobec dynamicznego rozwoju technologii, w tym tzw. sztucznej inteligencji można przewidywać, że instytucje obowiązane będą raczej zainteresowane w samodzielnej obsłudze funkcji związanych z bezpieczeństwem finansowym przy zastosowaniu zaawansowanych narzędzi technologicznych, niż w posiłkowaniu się wsparciem podmiotów trzecich, które i tak w myśl przepisów mają być traktowane jako część instytucji obowiązanej będąc podmiotem z nią zintegrowanym.

Nie może również pozostać bez komentarza fakt, że aby skutecznie powierzyć stosowanie niektórych środków bezpieczeństwa finansowego podmiotowi zewnętrznemu, instytucje obowiązane, takie jak przedstawiciele zawodów prawniczych, musiałyby ujawnić informacje uzyskane od klienta w związku z udzielaną pomocą prawną. W tym jednak zakresie powstają istotne wątpliwości,

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

gdyż o ile ustawowa możliwość przekazywania ich organom i agencjom bezpieczeństwa finansowego nie budzi wątpliwości, to udostępnianie ich podmiotom zewnętrznym może nie być objęte przepisami umożliwiającymi udostępnianie ich na podstawie przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Mateusz Ficygowski
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 5.

SHELL COMPANIES, OBOWIĄZKI INSTYTUCJI OBOWIĄZANYCH

5.1. UWAGI WSTĘPNE

Shell Companies są to podmioty istniejące tylko na papierze, nieposiadające rzeczywistych aktywów oraz nie zatrudniające pracowników. Brak możliwości zidentyfikowania firmy Shell Companies z rzeczywistą osobą zarządzającą jej aktywami narzuca problem z odpowiedzialnością. Firmy Shell są to korporacje-przykrywki zaangażowane w nielegalną działalność, potencjalnie niebezpieczne podmioty finansowe. Korporacje-przykrywki odgrywają ważną rolę na rynkach całego świata. Najczęstszym nadużyciem wykorzystywania firm Shell jest pranie brudnych pieniędzy oraz finansowanie terroryzmu.

Celem niniejszego rozdziału jest ukazanie złożoności spółek-przykrywek (Shell Companies) oraz wykorzystywania ich do nielegalnych czynności, takich jak pranie pieniędzy oraz finansowanie terroryzmu. Ponadto celem publikacji jest analiza instytucji obowiązanych w stosowaniu środków bezpieczeństwa finansowego w przypadku wykrycia uzasadnionego podejrzenia prania pieniędzy lub finansowania terroryzmu.

Instytucje obowiązane w swej działalności zajmują się przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu. Ustawa z dnia 18 marca 2018 r. wskazuje, jakie obowiązki ciążą na instytucjach obowiązanych. W szczególności ich zadaniem jest dokonanie analizy formalnej oraz materialnej zgromadzonego materiału na temat danego klienta.

Stosując środki bezpieczeństwa finansowego instytucje obowiązane w granicach swoich kompetencji mają obowiązek monitorowania wszelkich stosunków gospodarczych i transakcji każdego klienta. W szczególności, czy transakcje są

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

zgodne z aktualną wiedzą instytucji oraz czy dane są na bieżąco uaktualniane. W swej działalności dokumentują rozpoznane ryzyko, badając źródło pochodzenia, zakres prowadzonej działalności klienta, jednocześnie weryfikując jego tożsamość oraz stosunki gospodarcze z innymi podmiotami.

Codziennie w systemie bankowym są realizowane różnego rodzaju transakcje. Przeważająca część z nich nie należy do transakcji podejrzanych, są one legalnie podejmowanymi działaniami. Jednak pewna część z nich ma na celu pranie pieniędzy lub finansowanie terroryzmu. Takie transakcje są zaliczane do transakcji podejrzanych. Instytucje obowiązane stosując środki bezpieczeństwa finansowego mają obowiązek wstrzymania transakcji uzasadniających podejrzenie ryzyka nielegalnego procederu. Posiadana wiedza na temat nielegalnego procederu powinna być na tyle duża, że uzasadni podjęcie postępowania karnego wobec klienta. Rzetelne podejście instytucji obowiązanych przyczynia się do skutecznego zapobiegania praniu pieniędzy oraz finansowaniu terroryzmu. Za niedopełnienie należytej staranności instytucje podlegają sankcjom karnym, o których mowa w ustawie z dnia 18 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu i o których mowa w dalszej części rozdziału.

5.2. SHELL COMPANIES

W celu ukrycia struktur podmiotu gospodarczego, jakim jest pranie brudnych pieniędzy, wykorzystywane są najczęściej spółki, które nie prowadzą żadnej działalności gospodarczej ani też nie zatrudniają pracowników, a ich działalność skupiona jest tylko i wyłącznie na tym, aby pieniądze mogły zostać wprowadzone do obrotu. Według Komisji Europejskiej tworzone grupy trudniące się praniem brudnych pieniędzy kształtują coraz to nowe metody powstawania podmiotów gospodarczych (Shell Companies). Ukryte podmioty zazwyczaj mają siedzibę w innych krajach, a osoby, które występują w roli reprezentantów, są przykrywkami dla prawdziwych beneficjentów rzeczywistych. W rzeczywistości pozostają oni ukryci za „firmą przykrywką", a kluczowym elementem prowadzenia takiej działalności jest anonimowość[1].

Większość firm przykrywek może służyć legalnym celom, takim jak przechowywanie akcji lub aktywów. Mogą również skutecznie chronić tajemnice handlowe lub osoby, które z jakichś względów nie chcą się ujawniać. Firmy Shell mają podstawową cechę – zdolność do ukrywania prawdziwej własności oraz tożsamości. Z powodu ogólnego braku przejrzystości transakcji w branży firm przykrywek jest

[1] Ministerstwo Finansów, *Krajowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu*, , Lex/el, Warszawa 2019, s. 182.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

oczywiste, że osoby bezpośrednio uczestniczące w działalności nadużywają tych korzyści[2].

Od 1 marca 2018 r. w Polsce, zaczął obowiązywać Centralny Rejestr Beneficjentów Rzeczywistych (CRBR). Oznacza to, że beneficjenci przestają być anonimowi. Od momentu wejścia w życie CRBR wszystkie nowo powstałe spółki są obowiązane do wyjawienia swoich beneficjentów rzeczywistych. Warto dodać, że od kwietnia 2020 r. taki obowiązek ciąży również na podmiotach, które zostały założone przed dniem wejścia w życie obowiązku.

Spółki Shell tworzą złożone struktury korporacyjne. Spółki tego rodzaju są tworzone dużo wcześniej, aby instytucje były bardziej przychylne takim firmom. Spółki, które istnieją od wielu lat, są również bardziej atrakcyjne dla klientów, którzy chcą skorzystać z firm przykrywek. Takie spółki pozwalają w sposób wiarygodny ukryć lub przechować majątek przed wierzycielami, jak również wykorzystanie takich spółek pozwala partnerom biznesowym uprościć sprawy lub zagwarantować bezstronność prawną w jurysdykcji. Osoby uwikłane w konflikt z prawem, chcąc pozostać anonimowymi kupując grunty, nieruchomości itp. chowają swoją tożsamość właśnie za takimi spółkami przykrywkami[3]. Spółki Shell istnieją tylko z nazwy, zarejestrowane jako podmiot pomagają przestępcom uniknąć ściągania podatków, zwiększyć swoje zyski czy finansować dalszą działalność związaną z praniem pieniędzy lub finansowaniem terroryzmu. Największym problemem istnienia spółek Shell jest zagrożenie, gdy nie można ich powiązać z prawdziwą osobą czy osobami, które faktycznie nią zarządzają. Same firmy są bezwartościowe. Firma Shell może być wykorzystana do każdych celów[4]. Osoby kierujące firmą przykrywką, nie pozostawiają żadnych śladów, informacji oraz pozostają niezauważone. Najczęstszym wybieranym sektorem, w którym występują zjawiska prania pieniędzy, są przedsiębiorstwa, które zajmują się handlem towarami lub świadczące usługi, za które można płacić gotówką.

Shell Companies jest korporacją bądź firmą istniejącą tylko na papierze, nieposiadającą siedziby, miejsca oraz pracowników. Są to podmioty o nieistniejącej działalności i majątku, utworzone po to, aby ułatwić transfery wymiany walut bądź aktywów, bez generowania realnych zysków. Najważniejszym elementem działalności jest posiadanie konta bankowego.

Po przejściu wieloetapowego procederu prania pieniędzy odbywa się transfer pieniędzy w legalną sferę gospodarki. T. Pabiański zauważył, że Shell Companies są to podmioty, które zostały utworzone lub nabyte przez inne osoby odpowiedzialne za łańcuch całego aparatu łańcucha przestępczego. Istnienie ich może mieć na celu:

[2] J. Karin, *Spojrzenie za korporacje Shell*, SoFi, 27 lipca 2021.

[3] D. Jancisc, *Shell Companies and Government Coruption*, University Press, London 2018.

[4] LS. Duke, *Department sprawiedliwości Stanów Zjednoczonych, Spółki Shell, praktyki korporacyjne i jak je odkryć*, Griffin, Nashville 2019.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- znaczące utrudnienie pracy inspektorom skarbowym podmiotów odpowiedzialnych za pranie pieniędzy lub finansowania terroryzmu,
- produkowanie nieprawdziwych faktur, które mogą być ujęte przez podmioty za fakturę VAT stanowiące standardowe zakupy, a co za tym idzie, będą podstawą do naliczenia do obniżenia podatku za zobowiązanie podatkowe VAT.

Jednak unikanie opodatkowania jest czasami postrzegane jako luka w uchylaniu się od opodatkowania, ponieważ wiadomo, że korporacje te są wykorzystywane w działaniach na czarnym lub szarym rynku. Podejrzliwość wobec korporacji-przykrywki jest naturalna i ważne jest, aby zrozumieć różne scenariusze, w których powstają[5].

Na czele takich spółek stoją zazwyczaj osoby fizyczne, które nie istnieją. Są tak zwanymi „słupami" (ang. *Strawmen*). Osoby fikcyjne podpisują się pod wymaganymi dokumentami w zamian za określoną kwotę. Jest to niewielki procent w porównaniu do kwoty, która została wyłudzona z podatku VAT[6]. Wojewódzki Sąd Administracyjny w wyroku z dnia 6 maja 2016 r. o sygn. I SA/Kr 359/16 podkreślił, że fakt zawierania transakcji ze spółkami grupy Shell, nie narusza prawa, może to jednak wywoływać pewne wątpliwości dla organów, czy nie dochodzi do pomniejszenia należnych podatków VAT. Potwierdzenia wymaga zgromadzony materiał dowodowy, który jednoznacznie wskazywałby na sztucznie stworzoną spółkę, która ma na celu uzyskanie określonych korzyści podatkowych[7]. Korporacje Shell są wykorzystywane do wielu celów, niektóre są legalne, a inne nie. Chociaż potencjalnie niebezpieczne podmioty finansowe, korporacje-przykrywki odgrywają ważną rolę na rynkach całego świata. Biorąc pod uwagę ich międzynarodowy status i perspektywy wzrostu, należy stosować rygorystyczne strategie regulacyjne, aby zapewnić stabilność gospodarczą i bezpieczeństwo inwestorów w tej przestrzeni[8]. Głównym zagrożeniem firm Shell jest tajemnica otaczająca powłokę firm, która umożliwia im bycie narzędziem do unikania opodatkowania i prania brudnych pieniędzy. Możliwość zakładania i korzystania z firm przykrywek w celu uzyskania preferencyjnego traktowania przy umowach międzynarodowych, podatkowych, inwestycjach to również wielkie ryzyko. Anonimowość jest kluczowym elementem, który sprawia, że korzystanie z firm Shell jest atrakcyjne. Ważną funkcją jest to, że firma przykrywka zapewnia właścicielowi anonimowość przy jednoczesnym zachowaniu poufności oraz kontroli nad jej zasobami, aby działać bez kontroli ze strony organów ścigania. Potencjał anonimowości jest kluczowym czynnikiem ułatwiającym nadużywanie firm przykrywek.

[5] W. Kenton, M. Jomes, *Shell Corporation*, University Press, London 2020.

[6] T. Pabiański, W. Śliż, *Zorganizowane działanie przestępcze wykorzystujące mechanizmy konstrukcyjne podaktu VAT, cz. 1*, Wolters Kluwer, Warszawa.

[7] Wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 6 maja 2016 r. sygn. I SA/Kr 359/16.

[8] H. Kenin, *A look Behind Shell Corporation*, University Press, London 2021.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Gdy firmy przykrywki są wykorzystywane do unikania płacenia podatków w państwie, w którym są one należne, lub do unikania przepisów prawa pracy lub prawa socjalnego, podważają funkcjonowanie rynku wewnętrznego. Wpływa to negatywnie na PKB nie tylko z powodu utraty dochodów podatkowych, ale spadku wydajności iwzrostu nieuczciwej konkurencji. Ponadto może prowadzić do szerszych skutków politycznych i społecznych, takich jak rozwój działalności przestępczej, wzrost nierówności i zmniejszone zaufanie do instytucji publicznych[9]. Firmy Shell z natury są nielegalnymi podmiotami, są one jednak tworzone szybko w legalnym systemie i wykorzystywane jako narzędzie do nielegalnych procederów. Anonimowość związana z firmami-przykrywkami i celowe wysiłki przestępców w celu uniknięcia kontroli regulacyjnej mogą sprawić, że przestrzeganie AML będzie trudne. W związku z tym zespoły ds. zgodności z AML powinny być zaznajomione z cechami firm przykrywek, które mogą być wykorzystywane do prania pieniędzy. Monitorowanie transakcji firmy Shell można zidentyfikować na podstawie rodzajów transakcji, w które się angażują. Nietypowe wzorce transakcji lub transakcje z udziałem krajów wysokiego ryzyka mogą wskazywać na nadużycie firmy przykrywki[10].

Instytucje obowiązane zapobiegają unikaniu opodatkowania, praniu pieniędzy czy finansowaniu terroryzmu osobom zamieszanym w ten proceder, który jest dla nich priorytetem. Z ogólnego braku przejrzystości pochodzenia transakcji wskazują na oczywiste pochodzenie źródła z nielegalnego procederu. W celu ukrycia nielegalnych aktywów, ważne jest dla osób bezpośrednio zamieszanych w nielegalny proceder, aby firmy Shell Companies uniemożliwiły odkrycie osób bezpośrednio zaangażowanych. Patrząc z technicznego punktu widzenia, firmy Shell nie są nielegalnymi przedsiębiorstwami. Stają się nimi w momencie, gdy są wykorzystywane do prania pieniędzy czy finansowania terroryzmu, a rzeczywiste osoby unikają procesów sądowych.

5.3. INSTYTUCJE OBOWIĄZANE

W Polsce system przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu tworzą – instytucje centralne, instytucje obowiązane oraz instytucje współpracujące. Centralne instytucje nazywane są organami informacji finansowej, którymi są: Generalny Inspektor Informacji Finansowej, oraz minister właściwy do spraw instytucji finansowej. Ostatnim ogniwem systemu są jednostki współpracujące, czyli organy administracji rządowej i samorządu terytorialnego, inne państwowe

[9] I. KiendlKrišto, E. Thirion, *Ex-Post Evaluation Unit and European Added Value Unit*, EPRS, 2019.

[10] Brexit and AML/CFT, Shell Companies and Money Laundering.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

jednostki organizacyjne oraz Narodowy Bank Polski, Komisja Nadzoru Finansowego oraz Najwyższa Izba Kontroli[11].

Główną podstawą funkcjonowania aparatu zajmującego się przeciwdziałaniem praniu brudnych pieniędzy są podmioty, określane jako instytucje obowiązane. Ustawa z dnia 18 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w artykule 2 ust. 1 określa enumeratywnie katalog instytucji obowiązanych[12]. Zgodnie z tym artykułem ustawodawca wymienił podmioty, które w rozumieniu tej ustawy są owymi instytucjami obowiązanymi, czyli instytucjami, które są zobowiązane do wypełniania obowiązków przewidzianych w komentowanej ustawie. Porównując katalog instytucji obowiązanych z poprzednią ustawą z 2000 r., zaznaczyć należy, iż ustawodawca nie przeprowadził w tym zakresie kompleksowych zmian. W przeważającej mierze poprzedni katalog pokrywa się z obowiązującym katalogiem w znowelizowanej ustawie z dnia 18 listopada 2018 r. Zgodnie z obowiązującymi przepisami omawianej ustawy obowiązkiem instytucji obowiązanych jest prowadzenie bieżącego monitoringu stosunków gospodarczych, przede wszystkim badanie transakcji, które są dokonywane w trakcie stosunków gospodarczych, sprawdzanie, czy transakcje są zgodne z wiedzą instytucji obowiązanej na temat klienta oraz czy działalność i źródła pochodzenia środków, dokumentów oraz danych są na bieżąco uaktualniane. Jeżeli wystąpi sytuacja, że instytucja obowiązana nie będzie w stanie racjonalnie wyjaśnić działalności klienta, wówczas może to wskazywać na proceder prania pieniędzy lub finansowania terroryzmu. Poza analizą merytoryczną instytucje obowiązane mają za zadanie dokonać analizy formalnej, nakierunkowanej na badanie rzetelności danych oraz ich kompletności zawartych w rejestrze informacji o transakcjach[13]. Analiza powinna przede wszystkim podejmować identyfikację stron oraz wszelkie transakcje powinny być dokumentowane przez okres pięciu lat w formie pisemnej lub elektronicznej.

W momencie wejścia w życie ustawy z dnia 1 marca 2018 r., ustawodawca wprowadził do katalogu instytucji obowiązanych nowe podmioty. Nowym podmiotem ujętym w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu są podmioty, które świadczą usługi wymiany walut wirtualnych na prawne środki płatnicze, jak również dostawcy owych kont. W dyrektywie AML V w ósmym motywie preambuły można doczytać, że właściwe organy Państwowe powinny mieć możliwość monitorowania, jak są wykorzystywane wirtualne waluty. Jak również enumeratywnie w dziewiątym motywie preambuły wskazano,

[11] M. Capiga, *Bezpieczeństwo instytucji finansowych jako instytucji obowiązanych w systemie przeciwdziałania praniu pieniędzy*, „Studia Ekonomiczne" 2014, nr 171, s. 120–131.

[12] M.A. Kędzierski, *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce*, Wydawnictwo Adam Marszałek, Toruń 2019, s. 490.

[13] K. Grabowska, *MK Monitor księgowego wydanie specjalne. Przeciwdziałanie praniu brudnych pieniędzy oraz finansowaniu terroryzmu*, Inforlex, Warszawa 2019, s. 80.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

że jednostki analityki finansowej powinny mieć dostęp oraz możliwość zintegrowania wirtualnej waluty z tożsamością danego właściciela.

Największym problemem w związku z praniem pieniędzy oraz finansowaniem terroryzmu jest anonimowość wirtualnych walut. ustawodawca zawarł w przepisie artykułu 2 ust. 2 pkt 26 u.p.p.p. definicję waluty wirtualnej. Wskazał, że waluta wirtualna jest to „cyfrowe odwzorowanie wartości, które nie jest środkiem płatniczym emitowanym przez NBP".

Wskazany katalog instytucji obowiązanych nie rozwiązuje zupełnie problemu identyfikacji podmiotów, których działalność jest oparta na wirtualnych walutach. Problem powstaje chociażby w momencie, kiedy użytkownik walut może dokonywać transakcji bez pośrednictwa dostawców walut. Odnosząc się do wirtualnych walut, należy w pierwszej kolejności odróżnić waluty lokalne od walut wirtualnych. Waluty lokalne są to waluty, które są użytkowane tylko i wyłącznie na określonym terenie (mieście, regionie), korzysta z nich niewielka liczba osób, przez co zjawisko prania pieniędzy jest praktycznie znikome. Właścicielami walut lokalnych są zazwyczaj państwa. Wprowadzenie obiegu walut lokalnych ma za zadanie upłynnić przepływ gotówki w przeciwieństwie do walut wirtualnych. Ciekawostką jest, że Estonia zastanawiała się nad wprowadzeniem do obiegu waluty wirtualnej, ta waluta miała nazywać się „estcoins", jednak za namową banków odstąpiła od tej decyzji. Podstawowym powodem odstąpienia od wprowadzenia wirtualnej waluty było uznanie, że mogłoby to spowodować wzrost ryzyka prania pieniędzy[14].

Kolejnym podmiotem, który został objęty zakresem instytucji obowiązanych, są instytucje pożyczkowe. Zmianą, jaka w tej materii została dokonana, jest to, że instytucje pożyczkowe zostały objęte nadzorem KNF. Dzięki tej regulacji KNF jest uprawniony do podjęcia kroków w przypadku, gdy działalność owych instytucji budzi okoliczności, jakie mogłyby wskazywać jednoznacznie na nielegalne działanie oraz mogłoby to zagrażać interesom finansowym klienta. Komisja Nadzoru Finansowego może odmówić wydania zezwolenia na prowadzenie działalności pożyczkowej w przypadku niespełnienia podstawowych wymogów zawartych w artykule 59a z 12 maja 2011 r. o kredycie konsumenckim. Reasumując: powyższa zmiana jakiej ustawodawca dokonał, dodając na listę instytucji obowiązanych instytucje pożyczkowe, miała na celu niedoprowadzenie do powtórzenia się sytuacji, która miała miejsce w latach 2008–2009.

Ważną kwestią do wspomnienia jest również objęcie statusem instytucji obowiązanych spółek, które prowadzą depozyt papierów wartościowych. Oznacza to, że spółki te wykonują jedno z zadań „Krajowego Depozytu Papierów Warto-

[14] W. Kapica, J. Grynfelder, W. Ługowski, T. Mierzwiński, R. Obczyński, A. Otto, E. Patsiotos, Z. Piotrowska, A. Rycerski, J. Stolarczyk, *Przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu – komentarze praktyczne*, Wolters Kluwer, Warszawa 2020, s. 34–38.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ściowych". Prowadzenie takiego depozytu papierów wartościowych opiera się na określaniu ewidencji papierów wartościowych[15].

Ustawodawca umieścił również w katalogu instytucji obowiązanych przedsiębiorców, którzy swym działaniem świadczą usługi dla spółek i trustów. Analizując termin tych przedsiębiorców, należy zaznaczyć, że są to spółki, które swym działaniem świadczą kompleksowe usługi pod względem administracyjno-korporacyjnym. Podstawowym powodem ujęcia ich w niniejszym katalogu jest wykorzystywanie ich do ukrycia beneficjentów rzeczywistych. Prowadzenie rejestru umożliwia jednostkom obowiązanym analizowanie finansów oraz organów w spółce bez konieczności informowania jej o tym. Taka możliwość często zdaje się pomocna z uwagi na ryzyko obawy podjęcia przez organy czynności, które uniemożliwiłyby odkrycie czynności sprzecznych z prawem. Warto również zaznaczyć, że w związku z działalnością trustów zostali ujęci w katalogu instytucji obowiązanych – adwokaci, radcowie prawni, prawnicy zagraniczni, jak i doradcy podatkowi. Kwalifikacja wyżej wymienionych podmiotów do instytucji istnieje tylko w sytuacji, gdy świadczą oni na rzecz klienta określoną pomoc prawną lub doradztwo podatkowe w sferze:

- świadczenia pomocy przy umowach kupna–sprzedaży nieruchomości, ruchomości lub też kupna–sprzedaży przedsiębiorstw,
- świadczenia pomocy przy zarządzaniu środkami finansowymi lub aktywami,
- świadczenia pomocy przy zawieraniu umów bankowych, rachunków papierów wartościowych czy też wszelkiego rodzaju czynności związanych z ich prowadzeniem,
- świadczenia pomocy przy kapitalizowaniu spółek kapitałowych, w szczególności wnoszenia kapitału zakładowego, jego podwyższenia zgodnie z obowiązującymi przepisami kodeksu spółek handlowych,
- świadczenia pomocy prawnej przy tworzeniu spółek oraz ich zarządzaniu.

Wyjątkiem są adwokaci i radcowie prawni, którzy świadczą swą pomoc wykonując swój zawód na podstawie stosunku pracy w urzędach lub organach administracji rządowej[16]. Ustawodawca 30 marca 2021 r. uściślił również katalog instytucji obowiązanych doprecyzowując listę podmiotów:

- zgodnie z przepisami ustawy z dnia 6 marca 2018 r. Prawo Przedsiębiorców (Dz.U. z 2021 r., poz. 162)[17] przedsiębiorcy, których działalnością jest świadczenie usług z zakresu prawa podatkowego lub celnego m.in. sporządzanie deklaracji, prowadzenie ksiąg podatkowych oraz wyjaśnień z zakresu prawa podatkowego lub opinii,

[15] G. Blicharz, B. Oręziak, M. Wielec, *Rynek finansowy. Zapobieganie przyczynom przestępczości*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa 2019, s. 33–37.

[16] W. Kapica (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu, Komentarz*, Wolters Kluwer, Warszawa 2020, s. 41–42.

[17] Ustawa z dnia 6 marca 2018 r. Prawo Przedsiębiorców (Dz.U. z 2021 r., poz. 162).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- zgodnie z rozumieniem ustawy z dnia 21 sierpnia 1997 r. o Gospodarce Nieruchomościami (Dz.U. z 2020 r., poz. 11, 234 i 815)[18] pośrednicy w obrocie nieruchomościami,
- przedsiębiorcy w rozumieniu ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców, których działalność polega na obrocie, przechowywaniu dzieł sztuki, antyków oraz przedmiotów kolekcjonerskich.

Instytucje obowiązane w swej działalności podlegają sankcjom za niedopełnienie obowiązków. Przepis artykułu 147 u.p.p.p. wprowadza zakres kar administracyjnych przewidzianych przeciwko instytucjom obowiązanym za niedopełnienie obowiązków, jakie wynikają z ustawy. Kary pieniężne nakładane na instytucje są do wysokości dwukrotnej korzyści osiągniętej w wyniku naruszenia lub jeżeli nie da się ustalić, jaka została osiągnięta korzyść – do równowartości 1 000 000 euro. Argumentacją ustalenia wysokości oraz rodzaju kary są przede wszystkim:

- waga, jak również czas trwania przekroczenia uprawnień,
- odpowiedzialność instytucji w zakresie przekroczenia swoich uprawnień.

Stosownie do przepisu artykułu 150 ust. 1, ustawodawca wskazał katalog kar administracyjnych, jakie można nałożyć na instytucje obowiązane. Do katalogu kar administracyjnych zaliczamy:

- publikację informacji o instytucji obowiązanej oraz zakresie naruszenia przepisów ustawy przez tę instytucję w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych,
- nakaz zaprzestania podejmowania przez instytucję obowiązaną określonych czynności,
- cofnięcie koncesji lub zezwolenia albo wykreślenie z rejestru działalności regulowanej,
- zakaz pełnienia obowiązków na stanowisku kierowniczym przez osobę odpowiedzialną za naruszenie przez instytucję obowiązaną przepisów ustawy przez okres nie dłuższy niż rok,
- karę pieniężną[19].

Przy ustalaniu kary administracyjnej uwzględnia się:

- wagę naruszenia przepisów i czas ich trwania,
- zakres, w jakim instytucja ponosi odpowiedzialność za naruszenie przepisów,

[18] Ustawa z dnia 21 sierpnia 1997 r. o Gospodarce Nieruchomościami (Dz.U. z 2020 r., poz. 11, 234 i 815).

[19] Ustawa z dnia 1 marca 2018 r., o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723) art. 150 § 4.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- możliwości finansowe danej instytucji obowiązanej,
- wielkość korzyści lub uniknętej straty przez instytucję,
- niekorzystne skutki, jakie poniosły osoby trzecie w związku z naruszeniem przepisów instytucji,
- stopień współpracy instytucji z odpowiednimi organami do spraw przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu,
- czy miało miejsce wcześniej naruszanie przepisów przez instytucje[20].

Kwestią wartą uwagi jest, że karę pieniężną można nałożyć do dwukrotności kwoty, jaką instytucja obowiązana osiągnęła lub uniknęła straty w wyniku naruszenia, lub w przypadku, kiedy nie da się ustalić kwoty korzyści lub straty – do równowartości 1 000 000 euro[21].

Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu nakłada na instytucje obowiązane kompleksowe zbadanie ryzyka odnoszącego się do działalności danej instytucji, uwzględniając wszelkie czynniki ryzyka klienta, państwa, obszarów geograficznych, rodzajów usług czy transakcji. Działania te powinny być dostosowane do charakteru obowiązanej instytucji. W przypadku braku dopełnienia obowiązków nałożonych przez ustawę, instytucje obowiązane podlegają sankcjom karnym. Oprócz kar administracyjnych za niewłaściwe dopełnianie obowiązków grozi również odpowiedzialność karna.

5.4. ŚRODKI BEZPIECZEŃSTWA FINANSOWEGO

Państwa członkowskie Unii Europejskiej są zobligowane stosować mechanizmy, które są niezbędne do monitorowania oraz podejmowania niezbędnych środków do respektowania przepisów AML. W przepisie artykułu 130 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wskazuje podmiot, który jest odpowiedzialny za sprawowanie kontroli nad respektowaniem przepisów AML – jest to GIIF. Podstawowym założeniem przyznania nadzoru Głównemu Inspektorowi Informacji Finansowej było uniknięcie wielokrotnej kontroli przestrzegania przepisów, w której instytucje obowiązane miały dyspozycje kontrolować nawet w tej samej materii kilkukrotnie. Ustawodawca nie poprzestał tylko i wyłącznie na tej materii. Wskazał również inne podmioty, które sprawują nadzór w horyzoncie przestrzegania przepisów AML, są to:

- KNF (Komisja Nadzoru Finansowego) – w zakresie instytucji, które są przez nią nadzorowane,

[20] Ustawa z dnia 1 marca 2018 r., o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723, art. 150 4).

[21] K. Grajcar, *Limit płatności gotówkowych w świetle ustawy o przeciwdziałaniu praniu pieniędzy (AML)*, Wydawnictwo Naukowe Uniwersytetu Łódzkiego, Łódź 2021.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- naczelny urząd celno-skarbowy – w zakresie do instytucji, które są obowiązane do ich kontrolowania,
- prezes NBP – dotyczących osób, które prowadzą działalność kredytową w rozumieniu tej ustawy,
- prezesi sądów apelacyjnych – wobec notariuszy[22],
- Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa – wobec spółdzielczych kas oszczędnościowo-kredytowych,
- wojewodowie i starostowie – wobec stowarzyszeń, na zasadach sprecyzowanych w ustawie,
- ministrowie i starostowie – wobec fundacji, na zasadach sprecyzowanych w ustawie[23].

Ustawodawca w przepisie artykułu 33 ustawy u.p.p.p. wskazał, że instytucje obowiązane są zobligowane do stosowania wobec swoich klientów środków bezpieczeństwa finansowego[24]. Zgodnie z obowiązującymi przepisami ustawy instytucje obowiązane w swoich granicach mają obowiązek monitorowania stosunków pomiędzy podmiotami gospodarczymi, włącznie z transakcjami, których dokonują pomiędzy sobą, owych transakcji, czy są zgodne z aktualną wiedzą instytucji obowiązanej na temat rzeczonego klienta, postać działalności oraz występującej wątpliwości ryzyka, jak i w miarę możliwości, skąd pochodzą środki, jak są rozdysponowane oraz zapewnienia, że wszelkie posiadane dokumenty, informacje oraz dane są uaktualnione. Takie bieżące monitorowanie podmiotów ma na celu szybką reakcję na odbiegające od normy profile transakcyjne klienta[25]. Instytucje obowiązane do stosowania przepisów ustawy, stosując wobec swoich klientów środki bezpieczeństwa finansowego rozpoznają ryzyko, jakie powstaje w związku z praniem pieniędzy oraz finansowaniem terroryzmu. W swej działalności muszą udokumentować rozpoznane ryzyko uwzględniając takie czynniki jak:

- rodzaj potencjalnego klienta,
- na jakim obszarze dysponuje,
- jakie jest przeznaczenie rachunku,
- jaki jest rodzaj usług oraz produktów, które oferuje, oraz ich dystrybucja,
- jaka jest wartość przeprowadzonej transakcji kupna–sprzedaży,
- cel oraz regularność przeprowadzanych transakcji[26].

---

[22] M. Kędzierski, *Notariusz jako instytucja obowiązana w rozumieniu ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (omówienie niektórych zagadnień)*, „Studia Prawnicze KUL" 2020, nr 1, s. 165–195.

[23] W. Kapica, *op. cit*., s. 325–326.

[24] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723, art. 33).

[25] K. Grabowska, *op. cit*., s. 80–81.

[26] M. Brzostowska, M. Dziedźwiedzka, *Komentarz praktyczny, obowiązki biur rachunkowych w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu*, Lex/el, Warszawa 2021.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Oprócz powyższych kryteriów, które instytucje obowiązane powinny brać pod uwagę, jest też wiele czynników równie ważnych, zaleconych przez ustawodawca. Przy ocenie klienta ważną kwestią jest, czy jest on osobą fizyczną, czy też osobą prawną. W przypadku, jeżeli jest to osoba prawna, to w jakiej formie organizacyjnej została ona zawiązana oraz według jakiego prawa działa czy też jaka jest jej branża działania. Odnosząc się do obszaru geograficznego, w przypadku osób prawnych zwrócić uwagę należy na kwestie, w jakim państwie została ona utworzona, a w przypadku osób fizycznych gdzie została urodzona, jakiego jest obywatelstwa czy też jakie jest jej miejsce zamieszkania, miejsce wykonywania pracy lub aktywności osobistej. Kwestie rachunku również wymagają wielu dodatkowych szczegółów, przede wszystkim, jakie transakcje mogą być wykonywane przez klienta, czy będą to transakcje zagraniczne, krajowe czy wszystkie, jak również jaki jest to rachunek: czy na potrzeby osobiste, czy jest to podstawowy rachunek płatniczy. W odniesieniu do dystrybucji przyjmuje się, że zdalne kanały mogą generować podwyższone ryzyko prania pieniędzy lub finansowania terroryzmu, jeżeli ich ryzyko nie jest obniżone działaniami przez instytucje obowiązane. Ustawodawca wiąże przeprowadzone transakcje z poziomem wartości majątkowych klienta, im większa transakcja, tym większe ryzyko. Oczywistym jest, że wszelkie czynności klienta muszą zostać w prawidłowy sposób udokumentowane zarówno na potrzeby instytucji zewnętrznych, jak i kontroli wewnętrznej[27].

Warte uwagi jest również, że biura rachunkowe mają możliwość zastosowania środków bezpieczeństwa finansowego i z tego tytułu mogą przetwarzać zawarte w dokumentach informacje o kliencie oraz osobie, która jest upoważniona do jej reprezentacji, przy jednoczesnym poinformowaniu przed zawarciem transakcji gospodarczej klienta o przetwarzaniu jego danych osobowych, jak również o obowiązkach, jakie wynikają z ustawy i ciążą na instytucjach obowiązanych[28]. Podczas rozpoznawania ryzyka prania pieniędzy oraz finansowania terroryzmu środki bezpieczeństwa zgodnie z przepisem artykułu 34 u.p.p.p. obejmują:

- identyfikację klienta oraz weryfikację jego tożsamości,
- identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu:
  - weryfikacji jego tożsamości,
  - ustalenia struktury własności i kontroli – w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej,
- ocenę stosunków gospodarczych i, stosownie do sytuacji, uzyskanie informacji na temat ich celu i zamierzonego charakteru,
- bieżące monitorowanie stosunków gospodarczych klienta, w tym:

[27] W. Kapica, *op. cit.*, s. 105–108.

[28] M. Brzostowska, *Poradnik. Ocena ryzyka prania pieniędzy przez klientów biura rachunkowego*, Lex/el., 2021.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- analizę transakcji przeprowadzanych w ramach stosunków gospodarczych w celu zapewnienia, że transakcje te są zgodne z wiedzą instytucji obowiązanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz zgodne z ryzykiem prania pieniędzy, a także finansowania terroryzmu związanym z tym klientem,
- badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta – w przypadkach uzasadnionych okolicznościami,
- zapewnienie, że posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych są na bieżąco aktualizowane[29].

Instytucje obowiązane stosują katalog środków bezpieczeństwa finansowego, określonego w ustawie w każdym przypadku. Mają jedynie możliwość regulacji natężenia stosowania określonych środków bezpieczeństwa, w miarę rozpoznanego poziomu i ocenionego ryzyka[30]. W przepisie artykułu 35 u.p.p.p. został określony gruntowny wykaz sytuacji, które zostały skierowane do instytucji obowiązanych jako obowiązkowe stosowanie środków bezpieczeństwa finansowego. Są to:

- nawiązywanie stosunków gospodarczych,
- przeprowadzanie transakcji okazjonalnej o równowartości 15 000 euro lub większej bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza, czy kilka operacji, które wydają się ze sobą powiązane,
- przeprowadzanie transakcji okazjonalnej, która stanowi transfer środków pieniężnych na kwotę przekraczającą równowartość 1000 euro,
- podejrzenie prania pieniędzy lub finansowania terroryzmu,
- wątpliwość co do prawdziwości lub kompletności dotychczas uzyskanych danych identyfikacyjnych klienta,
- zmiana uprzednio ustalonego charakteru lub okoliczności stosunków gospodarczych[31].

Istnieją dodatkowo jeszcze dwie sytuacje stosowania oznaczonych środków bezpieczeństwa finansowego, które zostały zamieszczone w katalogu instytucji obowiązanych:

- w przypadku, gdy transakcja jest okazjonalna o równowartości 10 000 euro lub większej. Nie ma tu znaczenia, czy operacja została przeprowadzona pojedynczo, czy jest kolejną transakcją,
- wygrane, gdzie również nie ma znaczenia, czy transakcja jest pojedyncza, czy kolejną operacją, które mogą być ze sobą powiązane.

[29] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723, art. 34).

[30] M.A. Kędzierski, *op. cit.*, s. 607–610.

[31] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723, art. 35).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Podstawową zasadą instytucji obowiązanych jest stosowanie środków bezpieczeństwa finansowego w kwestii klienta oraz transakcji okazjonalnych[32]. Merytorycznym celem monitorowania jest niezwłoczne zidentyfikowanie klienta, który odbiega od rzeczywistej transakcji. Jeżeli instytucje obowiązane nie będą w stanie stwierdzić racjonalnie działalności, może to wskazywać na proceder prania pieniędzy lub finansowania terroryzmu. Instytucje obowiązane powinny również dokonać analizy formalnej nakierunkowanej na weryfikację danych oraz ich kompletności w rejestrze informacji o transakcjach[33]. Postanowienia dotyczące ustawy w kwestii środków bezpieczeństwa finansowego należy stosować w odpowiednim zakresie i intensywności oraz po uwzględnieniu rozpoznanego ryzyka w transakcjach czy stosunkach gospodarczych. W przypadkach, o których mowa w art. 43–46 u.p.p.p., powinny być stosowane „wzmożone środki bezpieczeństwa finansowego", a w szczególności, kiedy transakcje lub stosunki gospodarcze wynikają z nietypowych okoliczności i klientów, którzy pochodzą z krajów o podwyższonym ryzyku prania pieniędzy lub finansowania terroryzmu lub mających tam siedzibę[34]. Jednak sam system przeciwdziałania praniu pieniędzy pomimo rozbudowanych możliwości instytucji obowiązanych opiera na dwóch zasadniczych działaniach:

- gromadzeniu odpowiednich informacji na temat danego klienta,
- analizowaniu transakcji, które wzbudzają podejrzenie prania pieniędzy lub finansowania terroryzmu.

Działania te są dość zbliżone, jednakowo kiedy dotyczą one osób indywidualnych czy osób prawnych. Oczywistym jest, że jednak przy gromadzeniu informacji na temat osoby prawnej ma ono bardziej złożony charakter[35]. W sytuacji gdy klient unika kontaktu z instytucją obowiązaną lub odmawia wyjaśnień dotyczących źródeł pochodzenia transakcji czy majątku klienta oraz nie przedstawi w związku z tym stosownych dokumentów, instytucja obowiązana zawiadamia GIIF o okolicznościach, które mogą wskazywać na proceder prania pieniędzy lub finansowania terroryzmu. Ponadto w przypadku braku możliwości zastosowania przez instytucje obowiązane środków bezpieczeństwa finansowego, o których mowa w art. 34 ust. 1 u.p.p.p., instytucja obowiązana nie nawiązuje stosunków gospodarczych i nie przeprowadza transakcji[36]. Ważnym obowiązkiem instytucji obowiązanych

[32] W. Kapica, *op. cit*.„ s. 120–124.

[33] K. Grabowska, *op. cit*., s. 80–81.

[34] A. Golonka, *Przeciwdziałanie praniu pieniędzy w obliczu zmian wprowadzonych IV i V dyrektywą AML*, „Przegląd Ustawodawstwa Gospodarczego" 2020, nr 4.

[35] J. Grzywacz, *Skuteczność instrumentów przeciwdziałających w Polsce procederowi prania brudnych pieniędzy*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej w Płocku, Płock 2015.

[36] Komunikat nr 22 w sprawie praktycznych aspektów stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień, o których mowa w art. 74 i art. 86 ustawy AML.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

jest dokumentowanie stosowanych środków, ponieważ katalog środków musi zostać zastosowany w każdym przypadku. Istnieje jednak możliwość co do zasady manewrowania częstotliwością ich stosowania, a zakres będzie uzależniony od ryzyka, które dotyczy relacji z danym klientem.

5.5. TRANSAKCJE PODEJRZANE

Codziennie w systemie bankowym są realizowane różnego rodzaju transakcje. Przeważająca część tych transakcji jest typowana do transakcji z legalnie podejmowanymi działaniami. Pewna część tych transakcji wzbudza podejrzenia prania pieniędzy lub finansowania terroryzmu. Na instytucjach obowiązanych spoczywa obowiązek wychwycenia transakcji pod kątem oszustw[37]. Kontrole instytucji obowiązanych z oczywistych względów nie są w stanie wyłapać i przewidzieć każdej transakcji, które mają na celu proceder prania pieniędzy oraz finansowania terroryzmu. Instytucje obowiązane w swej działalności podczas typowania transakcji powinny być elastyczne oraz wciąż analizować zmieniające się warunki działania osób zamieszanych w działalność przestępczą. Należy jednak wymienić znaczące definicje transakcji.

- transakcje niejasne – wynikają z okoliczności, których nie da się jednoznacznie określić w kontekście ekonomiczno-finansowym, a w szczególności cel oraz realizacja nie jest w sposób wyczerpujący wyjaśniona,
- transakcje nietypowe – chodzi o transakcje, które nie są w żadnym stopniu podobne do innych transakcji realizowanych przez danego klienta. Między innymi nie są powiązane z zakresem oferowanych usług lub działalności klienta,
- transakcje nadzwyczajne – dotyczą one dużych kwot oraz nie da się ich wyjaśnić pod kątem gospodarczym. Są realizowane przez danego klienta w kosztowny sposób,
- transakcje powiązane – występują wtedy, kiedy dany klient realizuje transakcje w kilku operacjach często poprzez inne instytucje oraz oddziały, a ujawnione wskazują, że mogą one być ze sobą powiązane[38].

Nie ma znaczenia, czy informacje o transakcjach podejrzanych zostały uzyskane w trakcie kontroli, czy po jej zakończeniu. Po uzyskaniu informacji o zaistnieniu sytuacji podejrzenia prania pieniędzy lub finansowania terroryzmu instytucje obowiązane mają obowiązek wstrzymania takiej transakcji. Jeżeli jednak zaistnieje okoliczność braku możliwości wstrzymania takiej transakcji lub wstrzy-

[37] T. Kuijlen, G. Migut, *Wykrywanie nadużyć i pranie brudnych pieniędzy*, StatSoft 2004.

[38] Wolfsberg statement on AML Screening/Monitoring and Serching 2009, Grupa Wolfsberg 2009.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

manie mogłoby zaszkodzić wykryciu osób podejrzanych, instytucje obowiązane informują inne instytucje właściwe oraz instytucje analityki finansowej[39]. Kontrole instytucji obowiązanych mają za zadanie sprawdzić wnikliwie każdą transakcję, której równowartość przekracza 15 000 euro. Dodatkowo również w przypadku gdy więcej niż jedna operacja wskazuje, że są one ze sobą powiązane lub gdy transakcje wzbudzają podejrzenie prania pieniędzy lub finansowania terroryzmu. Rejestracja takiej transakcji odbywa się najpóźniej do następnego dnia roboczego. Ustalając, kiedy dana transakcja przekracza równowartość sumy euro, stosuje się średni kurs NBP dla danej waluty w dniu, kiedy transakcja jest dokonywana lub w dniu złożenia jej w depozycie przeprowadzania transakcji. Każdy takie rejestr jest wprowadzany do rejestru transakcji. Prowadzony jest w systemie informatycznym, umożliwiającym w razie potrzeby szybki odczyt. Każda transakcja zawiera niezbędne informacje, takie jak:

- datę, w której została przeprowadzona transakcja,
- dane osobowe, umożliwiające identyfikacje stron,
- kwotę oraz walutę, w której została przeprowadzona transakcja, jak również rodzaj tej transakcji,
- w przypadku uzasadnionego podejrzenia prania pieniędzy lub finansowania terroryzmu – miejsce, datę i sposób złożenia transakcji.

Do zadań instytucji należy również uwzględnienie ryzyka danego transferu, podczas monitorowania transakcji podejrzanych. Monitorowanie transakcji przez instytucje w szczególności powinny być dopasowane do działalności klienta, uwzględniając jego ryzyko na przestępcze działania[40]. Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. nie określa wprost pojęcia definicji „transakcji podejrzanej", wskazuje jednak na transakcje, które mogą mieć związek z tym procederem. Uzasadnienie podejrzenia powstaje wówczas, gdy zostaną spełnione przesłanki procederu z wysokim prawdopodobieństwem, że został spełniony czyn zabroniony, o którym mowa w art. 165 a lub 299 kodeksu karnego. Posiadana wiedza, musi być na tyle duża, że uzasadni podjęcie postępowania wyjaśniającego na podstawie kodeksu postępowania karnego, zgodnie bowiem z przepisem art. 17 § 1 pkt 1 kodeksu postepowania karnego nie wszczyna się postępowania a wszczęte umarza, gdy brak jest danych dostatecznie uzasadniających podejrzenie popełnienia przestępstwa. Sąd Najwyższy w wyroku z dnia 20 maja 2013 r. o sygnaturze III K 355/12 wskazał, że nie jest więc wystarczające ustalenie, że określone wartości majątkowe pochodzą z jakiejkolwiek czynności bezprawnej czy też nieujawnionego lub nielegalnego źródła. Nie jest także wystarczające w tym zakresie ogólne wskazanie, że korzyść

[39] P. Siejczuk, *Problematyka prania brudnych pieniędzy w regulacjach prawnomiędzynarodowych, europejskich i krajowych*, „Bezpieczeństwo Narodowe" 2012, nr III–IV (23–24), s. 212–214.

[40] J. Grzywacz, *op. cit.*

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

majątkowa pochodzi z działalności przestępczej, jakiegoś bliżej nieokreślonego czynu zabronionego czy też pewnej grupy przestępstw (np. przestępstw przeciwko mieniu czy oszustw podatkowych), bez sprecyzowania, o jaki konkretnie typ przestępstwa chodzi[41]. Rzetelne działania instytucji obowiązanych przy podejmowaniu czynności wobec klientów i ich transakcji przyczynia się do skutecznego zapobiegania praniu pieniędzy oraz finansowaniu terroryzmu, dlatego też instytucje obowiązane zapewniają w sposób przejrzysty i precyzyjny w swoich wewnętrznych regulacjach czynności w celu wyjaśnienia podejrzeń nielegalnego procederu. Wszelkie działania są dokumentowane w celu zapewnienia należytej staranności[42].

Ustawodawca nie określił w żaden sposób, w jaki ma być dokonywane przekazywanie przez instytucje obowiązane informacji na temat podejrzanych transakcji. Wskazał jedynie na zobligowanie ich do niezwłocznego przekazania takich informacji. GIIF wskazał na najważniejsze informacje, jakie powinny się znaleźć w treści:

- podstawowe dane:
  - szczegółowy opis transakcji, ze wskazaniem daty, kwoty, waluty oraz rachunków, które zostały wykorzystane do jej realizacji,
  - uzasadnienia podejrzenia prania pieniędzy lub finansowania terroryzmu,
  - dane wykorzystane do transakcji.
- dodatkowe dane:
  - informacje powiązane z wcześniejszymi informacjami przekazywanymi do GIIF,
  - schemat graficzny, w jakim pieniądze przepływają,
  - jeżeli da się określić, również dodatkowe dane o podmiotach z innych źródeł,
  - historie przelewów, rachunków,
  - informacje o zgromadzonych załącznikach[43].

W przypadku przekazywania do GIIF informacji o transakcjach, które mogą być niepełne z uwagi na fakt, że realizacja transakcji nie została zakończona, a instytucja obowiązana nie uzyskała jeszcze pełnej informacji na temat transakcji. W takiej sytuacji jest dopuszczalne przekazanie jedynie tych danych, które instytucja obowiązana posiada. W przypadku jednak danych identyfikujących strony transakcji, która została uznana za „podejrzaną" po jej przeprowadzeniu i w odniesieniu do której nie było obowiązku stosowania środków bezpieczeństwa finansowego, w tym identyfikacji i weryfikacji klienta – instytucja obowiązana może nie dysponować wszystkimi wymaganymi informacjami, o których mowa

[41] Wyrok Sądu Najwyższego z dnia 20 maja 2013 r., sygnatura akt III K 455/12.

[42] J. Rajewska, M. Strzelecka, *Praktyczne aspekty stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień*, Instytut Prawa, Bydgoszcz 2020.

[43] Generalny Inspektor Informacji Finansowej Komunikat GIIF dotyczący zasad rejestracji transakcji, 27 stycznia 2015.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

w art. 9 ust. 1 i 2 ustawy. Ponadto w przypadku niektórych kategorii transakcji, jak np. przelewów przychodzących z zagranicy, pomimo wystąpienia jednej z sytuacji obligującej do zastosowania środków bezpieczeństwa finansowego, instytucja obowiązana może nie posiadać wszystkich danych identyfikacyjnych stron transakcji. W takich okolicznościach jest dopuszczalne zarejestrowanie jedynie tych danych, które instytucja obowiązana posiada[44].

5.6. PODSUMOWANIE

Wykorzystywanie firm Shell Companies do nielegalnych celów jest powszechnie rosnącym zjawiskiem. Fakt, że zapewniają właścicielowi pełną anonimowość przy jednoczesnej pełnej kontroli nad sprawami organizacyjnymi, jest szczególnie atrakcyjny dla osób zamieszanych w proceder prania pieniędzy oraz finansowania terroryzmu.

Cel, jaki został założony podczas realizacji niniejszego rozdziału, został w znacznym stopniu osiągnięty. Firmy Shell niekoniecznie muszą stanowić ryzyko, jednak w oparciu o anonimowość i nadużywanie prawa są idealnym instrumentem od uchylania się od opodatkowania, a co za tym idzie, mogą źle wpływać na gospodarkę państwa, wzrost nieuczciwej konkurencji, rozwój działalności przestępczej oraz spadek zaufania do instytucji publicznych. Instytucje są obowiązane przeciwdziałać praniu pieniędzy stosując środki bezpieczeństwa finansowego.

Stabilne instytucje obowiązane umożliwiają bezpieczeństwo finansowe państwa. Głównym zadaniem instytucji jest rozpoznanie oraz ocenienie ryzyka związanego z praniem pieniędzy oraz finansowaniem terroryzmu. Na podstawie zebranych materiałów i ocenieniu ryzyka stosuje się środki bezpieczeństwa finansowego. W przypadku powzięcia informacji bezpośrednio wskazującej na nielegalny proceder instytucje obowiązane niezwłocznie przekazują informacje do GIIF.

Efekty przeciwdziałania praniu pieniędzy skłaniają do podstawowego wniosku, że niezbędna jest dokładna analiza każdej transakcji, w szczególności gdy transfery czy usługi pochodzą z krajów o podwyższonym ryzyku prania pieniędzy oraz finansowania terroryzmu. Przeprowadzenie merytorycznej oceny zebranego dowodu, który potwierdzi lub całkowicie wykluczy podejrzenie, jest zadaniem odpowiednich instytucji obowiązanych, stosujących środki bezpieczeństwa finansowego.

Celem stosowania środków bezpieczeństwa finansowego jest wykrywanie transakcji niejasnych oraz typowanie ich do odpowiednich kategorii. Jeżeli nie ma możliwości racjonalnego wytłumaczenia transakcji przez klienta lub transakcja odbiega znacząco od jego profilu, może to wskazywać na nielegalny proceder

[44] *Ibidem*.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

prania pieniędzy oraz finansowania terroryzmu. Należy przy tym pamiętać, że jeżeli brak jest wystarczających dowodów na stwierdzenie nielegalnego procederu, to zgodnie z przepisem artykułu 17 kodeksu postępowania karnego wszczyna się postępowania, a wszczęte umarza jeżeli brak jest wystarczających dowodów wskazujących na winę danego klienta.

Instytucje obowiązane w ramach swej działalności również podlegają sankcjom karnym za niedopełnienie obowiązków ustalonych przez ustawę.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Witold Wyporek
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 6.

FINTECH, GLOBALIZACJA USŁUG A KRAJOWE REGULACJE

6.1. UWAGI WPROWADZAJĄCE

Rozwój innowacyjności technologicznych stanowi szeroko pojmowane globalne zjawisko, a jego postęp nabrał doniosłego znaczenia w rozwoju gospodarek państw na całym świecie. Innowacyjność technologiczna umożliwia gospodarkom wykorzystanie nowych rozwiązań w odpowiedzi na potrzeby rynku i wizji nowej cyfrowej gospodarki. Sektor FinTech staje się coraz bardziej precyzyjnym przedmiotem zmian ustawodawcy krajów Unii Europejskiej. Zarówno globalnie, jak i w Europie czy też w Polsce doniosłe znaczenie z uwagi na innowacyjność zajmuje Sektor FinTech (Financial Technology)[1]. FinTech ogólnie sprecyzować można, jako nową gałąź gospodarki, której celem jest usprawnienie szeroko pojmowanych usług finansowych. W sektorze FinTech wykorzystywane są w wysokim stopniu technologie cyfrowe, dzięki czemu w przeważającym stopniu ma on największy wpływ na postęp gospodarki cyfrowej Polski[2]. Klasyfikacja Polski w zakresie wykorzystania nowych technologii plasuje się w czwartej ostatniej grupie wśród państw członkowskich z wynikiem 70% w zakresie zastosowania innowacyjności w latach 2014–2020. Natomiast jako państwo członkowskie, w którym najdynamiczniej wzrasta wskaźnik rozwoju wykorzystania innowacyjności, Polska zajmuje

[1] R. Milic-Czerniak, *Rola FinTechów w rozwoju innowacji finansowych,* Studia BAS, Biuro Analiz Sejmowych, Warszawa 2019, nr 1(57), s. 37–60.

[2] A. Alińska, *Alternatywne finanse,* Wydawnictwo CeDuWu, Warszawa 2019, s. 157–158.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

2. miejsce z wynikiem 14,6%, znajdując się za Chorwacją z wynikiem 21,5% w latach 2014–2021[3].

Podmioty obrotu gospodarczego inwestują w technologie finansowe podnosząc konkurencyjność i rozszerzając swoje oferty na nowo. Jednocześnie tworzą wewnętrzne struktury do zarządzania innowacyjną technologią począwszy od jej implementowania po zapewnienie realizacji wymogów ustawodawczych. Sektor FinTech z uwagi na różnorodność innowacyjności w nim wykorzystywanych i swoiste novum na globalnej arenie rozwoju gospodarek nie znajduje swojego utrwalonego kanonu prawnego. Znaczna część problematyki szczegółowej znalazła odzwierciedlenie w różnych aktach prawnych lub nie znajduje umocowania w ogóle. Do najważniejszych aktów prawa Unii Europejskiej niewątpliwie należy zaliczyć Dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego i Dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu.

Sektor FinTech obejmuje swoją definicją różne przedmioty działalności gospodarczej. Wśród nich należy wskazać produkty finansowe, usługodawców produktów finansowych i ich twórców, mechanizmy implementowania, rozpowszechniania i stosowania innowacji technologicznych, a także sektor, w którym innowacje te zachodzą. Celem nadrzędnym technologii finansowych jest uczynienie procesów gospodarczych i świadczenia usług bardziej sprawnymi, ekonomiczniejszymi i funkcjonalnymi. Pod pojęciem FinTech należy rozumieć podmioty obrotu gospodarczego świadczące innowacyjne usługi finansowe przy wykorzystaniu technologii informatycznych w sektorze finansów. W drodze wykorzystania innowacji technologicznych następuje zarówno tworzenie nowych usług, jak i zastosowanie nowych rozwiązań w już istniejących usługach. W sektorze FinTech funkcjonuje wiele podobnych do siebie rozwiązań rynkowych, różniących się od siebie pod względem wykorzystanej technologii i zastosowanych rozwiązań[4]. Rozwojowi sektora FinTech sprzyjają korzystne warunki dla łatwego implementowania innowacyjnych projektów. FinTech wyróżnia elastyczność w świadczeniu usług, tak aby możliwie jak najbardziej odpowiadała ona preferencjom klientów. Określając sektor FinTech można wymienić następujące podmioty[5].

- inicjowanie płatności – np. BLIK, PayPal, NicePay, Payto.app, autopay, GoPay, PayTel,
- e-bankowość i bankowość mobilna – iPKO, Millenet,

[3] European Innovation Scoreboard 2021 r., Luxembourg: Publications Office of the European Union, 2021, https://ec.europa.eu/docsroom/documents/46013 (data dostępu: 9 września 2021).

[4] O. Gawron, *Otoczenie regulacyjne sektora FinTech na przykładzie dyrektywy PSD2 i wybranych ustaw krajowych*, „Czasopismo Finanse i Prawo Finansowe" 2019, vol. 4(24), s. 49–65.

[5] Social.Estate, https://social.estate/slownik/FinTech-co-to-jest (data dostępu: 20 lipca 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- bankowość alternatywna – Varo, Chime, Nerdwallet, Revolut,
- kryptowaluty i wykorzystanie Blockchain – Bitcoin, Litecoin,
- usługi ubezpieczeniowe – Kundi, Mfid, protect.me, Boomerun, Link4, hiPRO,
- kredyty internetowe – Monero.pl, pluskantor, Bestekantor.pl, Liderwalut.pl,
- platformy pożyczkowe – TaniKredyt, Visset.pl, Pożyczko daj, Provema, Yolo, Wonga,
- kantory internetowe – np. Cinkciarz, Walutomatm, ik internetowy kantor, DobryKantor.pl,
- płatności HCE – Apple Pay, Google Pay,
- usługi przewozowe – e-hulajnoga, Uber, Bolt,
- zarządzanie finansami osobistymi – BillTech, Exerai, Cahap, Klasomat, Cube,
- usługi gastronomiczne – np. pyszne.pl,
- platformy zakupowo-zniżkowe, porównywarki cenowe, odroczone płatności-Twisto, Ceneo, Skąpiec, rankomat.pl, comperia, Porferl24.pl, Loando,
- sieci afiliacyjne – np. aff44,
- crowdfunding (finansowanie społecznościowe) – np. Beesfund, Patronite, Wspieram.to,
- cyberbezpieczeństwo – Esysco, Nethone, SigTech, Piwik,
- dostawcy oprogramowania – BeeiTech, GMP, Nextapps, Minisoftwere, Efigence,
- factoring – Brutto, Fandla, Faktoria, Finiata, Fundio, Monevia., Smeo, NFG,
- sztuczna inteligencja – Aibusters, Botwise, Digital Teammates, LogicAI, Self Learning Solutions.

Sektor FinTech można podzielić na zasadnicze dwa obszary działania (B2B – Business-to-business) i (B2C Business-to-consumer). W Sektorze B2B współpraca zachodzi w zakresie dostarczania usług o charakterze technologicznym, analitycznym, zapewniającym bezpieczeństwo i sprawność technologiczną świadczonym usługom w zarządzaniu bazami danych. W sektorze B2C wyznacznikiem jest dostarczenie usług do klientów w przystępnej formie, zapewniającej funkcjonalność i spełniającej oczekiwania, a także zapewnienie jej możliwie jak największej funkcjonalności[6].

Funkcjonowanie sektora FinTech odbywa się w ciągu nieustannych przemian ustawodawczych obejmujących coraz to nowe kwestie związane z tą technologią. Przepisy prawa odnoszące się do tych zagadnień są bardzo różne, mogą dotyczyć one samej formy działania FinTechów, jak np. startupy, albo obejmować nowe formy funkcjonalności technologicznej. Przykładowo można wskazać na technologie funkcjonujące w oparciu czy też wykorzystujące łańcuch DLTBlockchain. Warto w tym miejscu zaznaczyć, że prawo nie reguluje wielu kwestii związanych z FinTech, ponieważ innowacje technologiczne postępują z takim rozmachem, iż

[6] O. Gawron, *op. cit*., s. 49–65.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

prawo nie domaga w kompleksowym przystosowaniu do tych rozwiązań. Wobec wysoce rozwiniętej innowacji technologicznej na skalę globalną, wykorzystującej przy pomocy Internetu i urządzeń informatycznych technologie finansowe, w tym także rozwiązania oparte o zdecentralizowany rejestr DLT Blockchain gospodarki państw i organizacje w tym Unia Europejska dostrzegają potrzebę stworzenia trwałych prawnych unormowań na potrzeby zarówno funkcjonowania rynku, jak i ochrony podmiotów obrotu gospodarczego.

Ramy regulacyjne tworzone na potrzeby Sektora FinTech ujmowane są w sposób generalny i ogólny stanowiąc wyjściowe ramy prawne dla funkcjonowania. Oprócz tego można zaobserwować wpływ prawa soft law w postaci opinii rekomendacji i zaleceń, które nie mają charakteru wiążącego, natomiast mają istotne znaczenie dla funkcjonowania sektora, ponieważ ujmują one podejście do problematyki w sposób elastyczny. Urząd Komisji Nadzoru Finansowego opublikował w 2019 r. Cyfrową Agendę Rozwoju, która zakłada transformację cyfrową w oparciu o cyfrowe innowacje i stworzenie ram prawnych dla technologii innowacyjnej[7]. Warto także wskazać na Rezolucję Parlamentu Europejskiego z dnia 17 maja 2017 r. w sprawie FinTech. W dokumencie tym Parlament podkreśla, iż sektor FinTech wpływa pozytywnie na rozwój przedsiębiorstw finansowych i pośrednictwa. Natomiast podkreślono istotne zagrożenia związane z funkcjonowaniem tego sektora. Wiążą się one ze stabilnością finansową w kontekście wielu bilansów i raportów z wdrażania różnych regulacji prawnych. Wskazuje się na potrzeby nadzoru instytucji finansowych w zakresie uregulowania sektora pod kątem stabilności finansowej, a także potrzebę pełnych jasnych regulacji dotyczących danych, jakie mają być przekazywane instytucjom. Zagrożenia związane z bezpieczeństwem informatycznym i cyberbezpieczeństwem, a także potrzebę ochrony konsumentów. Rezolucja odnosi się także do problematyki łańcuchów blockchain i wykorzystania potencjału tej technologii w procesach i usługach o charakterze finansowym[8].

6.2. NADZÓR I KONTROLA SEKTORA FINTECH

Sektor Technologii Finansowych FinTech w przeważającej mierze jest sektorem krajowych instytucji płatniczych. Należą do niego instytucje zajmujące się usługami płatniczymi, które wyczerpują definicję podmiotową zawartą w ustawie z dnia 19 sierpnia 2021 r. o usługach płatniczych[9]. Na gruncie prawa Unii Europej-

[7] M. Nowakowski, *FinTech, technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji*, Wolters Kluwer, Warszawa 2020, s. 17–20.

[8] Rezolucja Parlamentu Europejskiego z dnia 17 maja 2017 r. w sprawie FinTech: wpływ technologii na przyszłość sektora finansowego (2016/2243(INI)) (Dz.U. UE. C. z 2018, nr 307, s. 57).

[9] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2020 r., poz. 794 z późn. zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

skiej aktem prawnym odnoszącym się do tych kwestii jest Dyrektywa Parlamentu Europejskiego i Rady UE 2015/2366 z dnia 25 listopada 2015 r.[10]. Dyrektywa usprawnia funkcjonowanie usług płatniczych w tym banków na model otwartej bankowości. Modyfikacjom ulegają także uprawnienia osób trzecich w zakresie dostępu do rachunków płatniczych i informacji o rachunku, a także wykonywania zleconych transakcji płatności i ich inicjowania, a ponadto usługę dostępności środków na rachunku. Zgodnie z dyrektywą w celu zezwolenia na działalność instytucji płatniczej wymagane jest złożenie odpowiedniego wniosku o zezwolenie do organów państwowych art. 5 dyrektywy[11]. Dodatkowym warunkiem jest posiadanie ubezpieczenia odpowiedzialności z tyt. prowadzenia działalności zawodowej. Udzielanie zezwoleń odbywa się jedynie w stosunku do osób prawnych mających siedzibę w państwie członkowskim, a uzyskanie zezwolenia może być poprzedzone konsultacjami z Bankiem Centralnym i innymi organami publicznymi art. 11 dyrektywy. Zapewnienie wymogów zgodnych z dyrektywą wymaga, aby wszystkie usługi płatnicze udostępniane drogą teleinformatyczną były bezpieczne, a ich zabezpieczenia gwarantowały bezpieczne uwierzytelnienie klienta, przez co zminimalizowane zostanie ryzyko oszustwa, wyłudzenia czy innego rodzaju przestępstwa[12].

Odzwierciedlenie tych wymagań znajduje swój wyraz w ustawie o usługach płatniczych[13]. Ustawa ta w sposób szczegółowy normuje kwestie świadczenia usług płatniczych, obrotu pieniądzem wirtualnym i kwestii związanych z transakcjami płatniczymi przy użyciu kart płatniczych. Art. 3 ust. 1 u.u.p. zawiera enumeratywnie wyliczony katalog usług płatniczych, w zakresie których znajdą zastosowanie przepisy ustawy wśród usługodawców. Głównym reżimem objęto wpłaty i wypłaty gotówki na rachunek płatniczy, wykonywanie transakcji płatniczych, usługi *acquiringu*, przekazy pieniężne i transakcje płatnicze (PIS), usługę (AIS)[14]. Oprócz organów administracji publicznej, banków krajowych i oddziałów banków zagranicznych, Europejskiego Banku Centralnego i instytucji w rozumieniu prawa bankowego dostawcami usług są również instytucje płatnicze, art. 4 u.u.p. Zgodnie

[10] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. UE. L. z 2015 r., nr 337, s. 35 z późn. zm.).

[11] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. UE. L. z 2015 r., nr 337, s. 35 z późn. zm.).

[12] K. Leżoń, *Otwarta bankowość w świetle wymogów Dyrektywy PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech*, Komisja Nadzoru Finansowego, Warszawa 2019, s. 17–19.

[13] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2020 r., poz. 794 z późn. zm.).

[14] B. Bajor (w:) *Ustawa o usługach płatniczych. Komentarz, wyd. II*, red. J. Byrski, A. Zalcewicz, Wolters Kluwer, Warszawa 2021, art. 3, s 143–155.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

z art. 60 u.u.p. usługi świadczone przez te podmioty wymagają uzyskania zezwolenia Komisji Nadzoru Finansowego. Zezwolenie wydawane jest po zaczerpnięciu opinii prezesa NBP, na którą składa się analiza zgodności wniosku z przepisami obowiązującego prawa i pod względem bezpieczeństwa usługi płatniczej art. 60 u.u.p.[15]. Przedmiotowa opinia jest wydawana w przeciągu miesiąca od otrzymania wniosku, natomiast samo postępowanie powinno zostać rozstrzygnięte w przeciągu 3 miesięcy. W przypadku konieczności uzupełnienia określonych w ustawie wymogów formalnych wniosku, przedłożenia dodatkowych informacji termin na wydanie zezwolenia zostaje wydłużony. Szczegółowe informacje w zakresie dokumentów i ich formy, jakie należy dołączyć do wniosku o wydanie zezwolenia, określa stosowne rozporządzenie[16].

Ustawa nakłada wymóg posiadania systemu zarządzania ryzykiem i kontroli wewnętrznej, koordynowania systemu i oceny funkcjonowania art. 64(a) u.u.p. System zarządzania ryzykiem i kontroli wewnętrznej jest strukturą organizacyjną wyposażoną w procedury decyzyjne w zakresie pełnego prowadzenia działalności gospodarczej. Procedury obejmują identyfikację ryzyka, oszacowanie jego skali, monitorowanie poziomu ryzyka i zarządzanie ryzykiem, w tym także ryzyka utraty płynności w zakresie udzielania pożyczek i kredytów. W skład systemu wchodzą także zasady i procedury instytucji obowiązanych w rozumieniu art. 2 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu[17]. Identyfikacja ryzyka pociąga za sobą również ryzyko operacyjne, bezpieczeństwo systemu, ochronę przed oszustwami, ryzyko prawne związane z charakterem zawieranych umów. Koniecznym jest również oszacowanie ryzyka związanego z aktualną sytuacją na rynku i płynnością finansową. W zakresie kontroli wewnętrznej prowadzone są audyty i kontrole zgodności z przepisami prawa prowadzonej działalności i świadczonych usług. Jednym z głównych elementów kontroli i audytu jest badanie zgodności działalności instytucji płatniczej z ustawą o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu[18].

W zakresie usługodawców sektora FinTech uprawnione są także do prowadzenia działalności gospodarczej podmioty zagraniczne. Działalność podmiotów zagranicznych stanowi niezwykle istotny element na polskim rynku. Europejski Urząd Nadzoru Bankowego współpracuje z Komisją Europejską na rzecz uspraw-

[15] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2020 r., poz. 794 z późn. zm.).

[16] Rozporządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 13 listopada 2020 r. w sprawie szczegółowego zakresu informacji oraz rodzaju i formy dokumentów dołączanych do wniosku o wydanie zezwolenia na prowadzenie działalności w charakterze krajowej instytucji płatniczej (Dz.U. z 2020 r., poz. 2225).

[17] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2021 r., poz. 1132 z późn. zm.).

[18] A. Zalcewicz (w:) *Ustawa o usługach płatniczych. Komentarz*, wyd. II, red. J. Byrski, Wolters Kluwer, Warszawa 2021, art. 64(a), s. 554–566.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nienia działalności transgranicznej FinTechów. Uprawnienie do prowadzenia działalności za granicą odbywa się na mocy wydanego zezwolenia KNF. Świadczenie usług może następować w drodze wykonywania pracy przez agenta, funkcjonowania oddziału czy też działalności transgranicznej. Instytucja obowiązana jest do zawiadomienia o zamiarze prowadzenia usług na terytorium innego państwa członkowskiego art. 92 u.u.p.[19]. Zawiadomienie musi także zawierać informacje o mechanizmach kontroli w zakresie opisu kontroli wewnętrznych, o którym mowa w ustawie o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Zawiadomienie musi zawierać m.in. opis struktury organizacyjnej oddziału, program i plan działania, zdefiniowane mechanizmy kontroli wewnętrznej.

Działania nadzorcze w zakresie funkcjonowania krajowych instytucji płatniczych sprawowane są przez KNF, stosownie do art. 99 i kolejnych ustawy u.u.p. Celem działań nadzorczych KNF jest zapewnienie bezpieczeństwa finansowego i zgodności podejmowanych działań krajowych instytucji płatniczych, a także ochrona interesów posiadaczy i użytkowników pieniądza elektronicznego. Niezbędnym wobec powyższych wymagań jest właściwa ocena instytucji płatniczej pod względem jej zdolności finansowej, sprawowania zarządu i kontroli wewnętrznej instytucji. Zakres nadzoru KNF określa szczegółowy katalog uprawnień w art. 102 u.u.p., na mocy których komisja podejmuje działania. Na szczególną uwagę zasługuje zobowiązanie instytucji w określonym terminie do udzielenia konkretnych informacji, żądanie przedkładania danych okresowych na potrzeby dokonania oceny pod względem finansowym instytucji płatniczej. Wydawanie zaleceń, nakaz wstrzymania wypłat z zysku i tworzenia nowych jednostek organizacyjnych. Nakaz sporządzania planu przywracającego prawidłowe funkcjonowanie jednostki[20]. Ponadto KNF uprawniony jest do kontroli zarówno działalności, jak i finansowej sytuacji KIP, art. 103 u.u.p. W ramach tych uprawnień KNF może dokonać wstępu do pomieszczeń, wglądu w dokumenty i dane, w tym także dane teleinformatyczne art. 103 ust. 4 u.u.p.[21]. Wreszcie stosownie do art. 105 u.u.p. w przypadku stwierdzenia, że KIP nie wypełnia obowiązków nałożonych ustawą, a także w przypadku stwierdzenia, iż działalność tych instytucji następuje z naruszeniem prawa lub stanowi zagrożenie interesu użytkowników, KNF może podjąć konkretne działania. Zgodnie z art. 105 u.u.p. KNF uprawniony jest do wystąpienia o odwołanie osoby ponoszącej odpowiedzialność za nieprawidłowości, zawieszenia w czynnościach osoby zarządczej, nałożenia ograniczenia na zarządzającego, a także wystosowania kary pieniężnej. W stosunku do osoby odpowiedzialnej za nieprawidłowości w wysokości do trzykrotności uśrednionego wynagrodzenia miesięcznego tej osoby, a w stosunku do samej KIP karę w kwocie do 1 000 000 zł

[19] M. Nowakowski, *op. cit.*, s. 80–81.

[20] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2020 r., poz. 794 z późn. zm.).

[21] M. Nowakowski, *op. cit.*, s. 82–85.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

art. 105 ust. 2 kpt. 5 u.u.p. Wymierzając karę pieniężną KNF bierze pod uwagę rodzaj i wagę naruszonych przepisów prawa, a także wymiar działalności KIP i jej sytuację finansową art. 105 ust. 2 u.u.p.[22].

Urząd Komisji Nadzoru Finansowego w swoich strukturach posiada komórkę organizacyjną w postaci Departamentu Innowacji Finansowej FinTech, któremu powierzono prowadzenie spraw związanych z sektorem FinTech[23].

6.3. RYZYKO USŁUG SEKTORA FINTECH A PRZECIWDZIAŁANIE PRANIU PIENIĘDZY I FINANSOWANIU TERRORYZMU. *ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM* (AML/CFT)

Doniosłe znaczenie w dla sektora FinTech mają przepisy prawa Unii Europejskiej w sprawie wykorzystania systemu finansowego do prania pieniędzy lub finansowania terroryzmu ujęte w dyrektywie Parlamentu Europejskiego i Rady UE 2015/849 z dnia 20 maja 2015 r. Państwa członkowskie są obowiązane do zapewnienia wymagań dyrektywy w celu zapobiegania wykorzystaniu systemu unijnego do działań przestępczych, art. 1 dyrektywy. Zjawisko prania pieniędzy zostało zdefiniowane w dyrektywie jako umyślne czyny polegające na przekazywaniu mienia pochodzącego z działalności przestępczej, obracaniu nim lub częścią jego udziału, ukrywanie lub zatajanie pochodzenia, źródła mienia, własności. Praniem pieniędzy jest także świadome nabywanie, wejście w stan posiadania, jak również udział, współudział, pomocnictwo i usiłowanie popełnienia czynów wymienionych w art. 1 lit. a–c[24]. Dyrektywa znajduje zastosowanie do podmiotów zobowiązanych państw członkowskich wymienionych w art. 2. Przykładowo interpretacja art. 2 w zw. z art. 3 pkt. 7 lit. dyrektywy stanowi o obowiązywaniu tych przepisów nie tylko w stosunku do spółek prawnych i innych osób prawnych, ale także osób prawnych, których przedmiotem działalności jest sprzedaż utworzonych wyłącznie

[22] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2020 r., poz. 794 z późn. zm.).

[23] Zarządzenie nr 5/2021 Przewodniczącego Komisji Nadzoru Finansowego z dnia 22 lutego 2021 r., w sprawie nadania regulaminu organizacyjnego Urzędowi Komisji Nadzoru Finansowego.

[24] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. UE. L. z 2015 r., nr 141, s. 73 z późn. zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

w celu zbycia spółek[25]. Wśród innych podmiotów objętych dyspozycją art. 2 dyrektywy znajdują się instytucje kredytowe, a także finansowe, osoby fizyczne i prawne m.in. notariusze, podmioty świadczące usługi handlem towarami, zajmujące się turystyką, handlem dziełami sztuki, wymianą walut wirtualnych i obrotem walutami wirtualnymi, dostawcy kont waluty wirtualnej. Notariusze obowiązani są do rejestracji transakcji o wartości przekraczających 15 000 euro, a także transakcji darowizny. Podczas darowizny nie dochodzi co prawda do transferu środków pieniężnych, ale ma miejsce transfer wartości majątkowych, a zatem instytucja ta może być wykorzystywana do prania pieniędzy[26]. Państwa członkowskie zobowiązane są dokonywać analizy ryzyka zakresu zawartego w sposób wyrażony w dyrektywie lub w sposób rozszerzający, o czym w zakresie poszerzonego zakresu stosowania należy poinformować komisję (art. 4). Celem zapewnienia należytych standardów ochrony zgodnie z art. 5 państwa członkowskie uprawnione są do stosowania zaostrzonych przepisów niż wyrażone w dyrektywie (art. 5). Państwa obowiązane są do stosownych działań celem identyfikacji, oceny i minimalizowania ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu. Ocena ryzyka sporządzona przez państwa członkowskie jest na bieżąco aktualizowana (art. 7). Kontrola ryzyka dokonywana jest w drodze powołanego organu na szczeblu każdego państwa, z czego należy przedłożyć informację komisji. Komisja dokonuje oceny ryzyka rynku wewnętrznego Unii Europejskiej, także w zakresie transgranicznym, sporządzając stosowne sprawozdanie aktualizowane co 2 lata (art. 6).

Zadaniem nałożonym na państwa UE jest zagwarantowanie utrzymania wysokich standardów identyfikacji, oceny i ryzyka przez instytucje zobowiązane, a także weryfikacja w zakresie czynników występującego ryzyka o zasięgu globalnym, tj. u podmiotów państw trzecich. Szczególnie w zakresie handlu wymiany usług, dokonywania transakcji itp. W zakresie występującego ryzyka państwa członkowskie gwarantują podejmowanie stosownie adekwatnych do wielkości i charakteru działań w tym zakresie przez zobowiązane na szczeblu krajowym podmioty[27].

Zakresem przedmiotowym problematyka prania pieniędzy i finansowania terroryzmu unormowana została w prawie krajowym ustawą z dnia 1 marca 2018 r.

[25] C-676/16, działalność gospodarcza polegająca na sprzedaży spółek utworzonych wyłącznie w celu ich zbycia, a przeciwdziałanie korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu., Corporate Companies s.r.o. v. Ministerstvo Financí ČR – Wyrok Trybunału Sprawiedliwości.

[26] II GSK 1996/12, obowiązek rejestracji transakcji umów darowizny nieruchomości. Wykorzystanie transakcji darowizny nieruchomości w procesie prania pieniędzy – Wyrok Naczelnego Sądu Administracyjnego.

[27] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. UE. L. z 2015 r. nr 141, s. 73 z późn. zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

o przeciwdziałaniu praniu pieniędzy i finansowania terroryzmu[28]. Normatywny charakter problematyki zawarto w przepisach ustawy karnej wyodrębniając zjawisko prania pieniędzy i finansowania terroryzmu. Określono szczegółowe znamiona czynów zabronionych, stosownie do art. 165a i art. 299 k.k.[29]. Dokonanie czynu zabronionego może nastąpić zarówno z zamiarem ewentualnym, jak i bezpośrednim[30]. Zamiar sprawcy czynu musi występować w zakresie wszystkich znamion określonych w art. 299 k.k. Wiedza sprawcy w zakresie kwalifikacji prawnej czynów stanowiących o podstawie pochodzenia pieniędzy jest nieistotna. W zakresie kwalifikacji art. 299 k.k. wystarczająca jest jedynie świadomość, iż źródłem pochodzenia pieniędzy są przestępstwa[31]. Przedmiot przestępstwa w rozumieniu art. 299 k.k. stanowią zarówno środki pochodzące bezpośrednio, jak i pośrednio z dokonanego czynu zabronionego[32]. Warto w tym miejscu podkreślić, iż czyny z tych artykułów są przestępstwami w rozumieniu ustawy kodeks karny, a dodatkowo stanowią one delikty administracyjne, na podstawie rozdziału 13 szczegółowej ustawy krajowej o praniu pieniędzy i finansowaniu terroryzmu.

Funkcjonowanie sektora FinTech objęte przepisami dyrektywy AML stanowi ryzyko w zakresie stabilności i wiarygodności systemu finansowego, a także integralności tego systemu na szczeblu UE. W zakresie tych regulacji zastosowanie znajduje ustawa krajowa, która wdraża przepisy unijne zarówno w zakresie państwa członkowskiego jako podmiotu obowiązanego w strukturach Unii Europejskiej, obok funkcjonowania przepisów krajowych w zakresie działań o charakterze przestępczym, a także ustawa odnosi się do samych instytucji zobowiązanych w zakresie nałożonych na nie obowiązków, kontroli i nadzoru w tym zakresie po kary administracyjne.

Następnie w art. 2 ustawy mamy do czynienia z enumeratywnie wymienionym katalogiem podmiotów obowiązanych, tzw. instytucji finansowych obowiązanych w tym także FinTechów wobec wymogów nałożonych przedmiotową ustawą. Wskazać należy, iż wśród instytucji obowiązanych ustawodawca umieścił także usługodawców wymiany waluty wirtualnej i fiducjarnej, dostawców kont walut wirtualnych. Stanowi to ważny element w walce i identyfikacji ryzyka prania pieniędzy, ponieważ podmioty rynku finansowego świadczące usługi z zakresu obrotu walutami wirtualnymi podlegać będą instytucjom kontroli. Ustawodawca niewątpliwie wprowadził regulacje będące odpowiedzią na źródło jednego z głów-

[28] Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r., poz. 815).

[29] Ustawa z dnia 19 kwietnia 1969 r. Kodeks karny (Dz.U. z 1969 r., nr 13, poz. 94).

[30] II AKa 163/16, Strona podmiotowa prania pieniędzy – Wyrok Sądu Apelacyjnego w Gdańsku.

[31] II AKa 42/17, Śmierć oskarżonego po wydaniu wyroku. Świadomość przestępczego pochodzenia pieniędzy jako warunek odpowiedzialności za pranie pieniędzy – Wyrok Sądu Apelacyjnego w Katowicach.

[32] II AKa 150/14, Przedmiot prania pieniędzy. Zakres zakazu prowadzenia działalności gospodarczej, Wyrok Sądu Apelacyjnego w Poznaniu.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nych zagrożeń prania pieniędzy, ponieważ w drodze obrotu walutami wirtualnymi przy zachowaniu wysokiego stopnia anonimowości dochodzi do nielegalnych transferów i podejrzanej wymiany, a także kradzieży i wyłudzeń. Przeważająca ilość zjawisk kryminogennych w zakresie obrotu walutami wirtualnymi odbywa się w szarej strefie poza zakresem ustawodawcy, jednakże wprowadzenie tych zmian odnosi się w sposób pośredni do sektora FinTech, świadczącego usługi w zakresie obrotu wymiany i prowadzenia kont waluty wirtualnej[33]. Ustawa nakłada wobec instytucji obowiązanych wymóg zatrudniania kadry ponoszącej odpowiedzialność za wypełnienie wymagań nałożonych ustawą w zakresie funkcjonowania jednostki art. 6 u.p.p.p. Ustawodawca posłużył się pojęciem kadry kierowniczej wyższego szczebla, przez co należy rozumieć, że personel ten będzie kompetentny w sprawach wiążących instytucję z uwagi na przepisy AML. Dodatkowo ustawodawca wymaga stanowiska zajmującego się wdrażaniem wymogów ustawodawcy, a także stanowiska nadzorczego w zakresie zgodności funkcjonowania podmiotu zobowiązanego z przepisami ustawy o praniu pieniędzy, art. 7 i 8 u.p.p.p., Approved AML Compliance Officer (AMLCO). Umocowanymi organami do informacji finansowej są zgodnie z art. 10 ustawy Minister Właściwy do spraw Finansów Publicznych, Główny Inspektor Informacji Finansowej[34]. Na szczególną uwagę w kontekście sektora FinTech należy zwrócić uwagę przy art. 12 u.p.p.p., który stanowi rozbudowany katalog zadań GIIF. W zakresie swoich kompetencji inspektor może dokonywać m.in. analizy informacji majątkowych, wstrzymywania transakcji i blokad rachunku, żądać informacji, kontrolować zgodność z przepisami prawa, wydawać decyzje o wpisie na listę podmiotów, w zakresie których zastosowanie znajdują szczególne środki ostrożności. Ważnym uprawnieniem inspektora jest także nakładanie kar administracyjnych, a także inicjowanie innych działań celem przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Przykładowo GIIF po przeprowadzeniu trwającej 9 miesięcy kontroli w spółce organ nałożył karę pieniężną w wysokości 600 000 zł tytułem niewyznaczenia osoby odpowiedzialnej na podstawie art. 8 u.p.p.p., brak procedur wewnętrznych na podstawie art. 50 i 53 u.p.p.p., brak sporządzonej oceny ryzyka art. 27 u.p.p.p., brak wystarczających środków bezpieczeństwa finansowego[35]. GIIF współpracuje także z organami administracji rządowej i samorządu terytorialnego, jak również z innymi podmiotami NBP, KNF, NIK. Stosownie do art. 14 u.p.p.p. GIIF składa na ręce Prezesa Rady Ministrów roczne sprawozdanie z działalności w terminie 3 miesięcy do końca roku kalendarzowego[36].

[33] *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu, Komentarz*, red. W. Kapica, Wolters Kluwer, Warszawa 2020, s. 35–38.

[34] *Instrukcje księgowe i podatkowe*, red. A. Hołda, wyd. 2, C.H. Beck, Warszawa 2020, s. 1318–1324.

[35] VI SA/Wa 2690/20 – Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie.

[36] Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r., poz. 815).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Urząd GIIF wyposażony jest w instytucję pomocniczą, którą jest KBF Komitet Bezpieczeństwa Finansowego, do którego zadań należy opiniowanie i doradztwo w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Zadaniem KBF jest także opiniowanie krajowej oceny ryzyka prania pieniędzy i planów strategicznych ograniczenia ryzyka prania pieniędzy nakierowanych na przestępstwa. KBF rekomenduje i opiniuje stosowanie szczególnych środków ograniczenia wobec osób fizycznych i innych podmiotów, art. 19 u.p.p.p.[37].

Sprawozdanie, o którym mowa w art. 14 u.p.p.p. opublikowane zostało przez GIIF w BIP w 2021 r. W sprawozdaniu tym GIIF podkreśla, iż podmioty obowiązane, instytucja GIIF i jednostki współpracujące działają w sposób oddziałujący na siebie, od czego zależy wynik efektywności ich działania. Wśród jednostek współpracujących należy wymienić organy rządowej administracji państwowej, jednostek samorządu terytorialnego. W szczególności Policja, CBA, ABW, SG, Prokuratura Krajowa, Krajowa Administracja Skarbowa, NIK, NBP, KNF, a także zagraniczne jednostki analityki finansowej. Dane przekazywane do GIIF są analizowane i weryfikowane w zakresie podejrzenia popełnienia przestępstwa w zw. z praniem pieniędzy lub finansowaniem terroryzmu, a następnie kierowane do prokuratury. Następnie podejmowane są działania prokuratora przy współpracy z organami ścigania, celem przedstawiania aktu oskarżenia. Sprawozdanie wskazuje, iż w 2020 r. odnotowano 3805 podejrzanych transakcji zgłoszonych do GIIF, które zostały poddane szczegółowej analizie organu. W porównaniu z latami sprzed 2012 r. jest to w dalszym ciągu wysoki poziom zgłoszeń, który stanowi powyżej 3500 podejrzeń od 2016 r. Wśród przesłanek stanowiących o zgłoszeniu do GIIF w przeważającej mierze w liczbie 3172 zgłoszeń stanowiły powiadomienia od instytucji obowiązanej na podstawie art. 74 u.p.p.p.[38]. Za okoliczności, które uznać należy jako uzasadnienie w zakresie prania pieniędzy i finansowania terroryzmu to nietypowe transakcje, budzące wątpliwości, nieklarowne, niezwykłe, rzadkie, nieprzeciętne, wyjątkowe z jakiegoś powodu[39]. Szczególnie pomocne w zakresie podejrzenia prania pieniędzy mogą być praktyki kwalifikacji z uwagi na transakcje przeprowadzone na zewnątrz działalności instytucji i klienteli, podjęcie współpracy z nowymi podmiotami zagranicznymi i porzucenie współpracy krajowej. Niekonwencjonalne decyzje finansowe, np. brak tytułów prawnych dokonanych transakcji, prowadzenie rachunku bankowego w miejscu nie mającym znaczenia dla prowadzonej działalności gospodarczej. Miarodajne dla zgłoszenia przez instytucję jest opisanie okoliczności i uzasadnienie podejrzenia budzącego wątpliwości. Ustawa w art. 14 u.p.p.p. nie precyzuje konkretnie katalogu dowodów, które

[37] https://www.gov.pl/web/mswia/giif.

[38] Sprawozdanie Głównego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2020 r., Warszawa 2021, s. 20–35.

[39] R. Lizak, *Pranie pieniędzy w prawie polskim na tle europejskim, międzynarodowym i amerykańskim,* C.H. Beck, Warszawa 2018, s. 240–243.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

świadczą o transakcji podejrzanej. Z uwagi na to należy stwierdzić, iż źródłem podejrzenia może być każda rzetelna i prawdziwa informacja budząca realne jak to ujmuje ustawa podejrzenie popełnienia przestępstwa. Stosownie do art. 74 ust. 2 u.p.p.p. zgłoszenie powinno być dokonane niezwłocznie, nie później niż w ciągu 2 dni roboczych[40].

W pozostałym zakresie transakcje podejrzane stanowiły powiadomienia jednostek współpracujących w zakresie art. 86, 90, 89, jak również jednostek współpracujących na podstawie art. 83 u.p.p.p. i inne.

Ponadto do podstawowych zadań GIIF należy analizowanie informacji o transakcjach w szczególności ponadprogramowych art. 72 u.p.p.p. Z tego tytułu do GIIF w 2020 r. wpłynęło 33,37 mln transakcji ponadprogramowych, które analizowane są i archiwizowane w Departamencie Informacji Finansowej Ministerstwa Finansów. Zakres przedmiotowy raportów określa ustawa, należą do nich wpłaty i wypłaty środków w gotówce, transfery środków finansowych, transakcje kupna sprzedaży środków dewizowych, a także niektóre czynności notarialne[41].

Podmioty sektora FinTech obowiązane są, podobnie jak inne instytucje obowiązane, do stosowania środków bezpieczeństwa finansowego. W zakresie prowadzonej przez siebie działalności klasyfikują ryzyko prania pieniędzy i oceniają jego poziom. Ponadto ustawa nakłada także obowiązek dokumentowania zakwalifikowanego ryzyka i jego oceny. W zakresie gromadzonych danych ustawa wymienia takie informacje, jak dane o kliencie, położenie geograficzne, dane o rachunku, dane o produkcie i jego wartości art. 33 u.p.p.p. Przy klasyfikacji ryzyka w gestii podmiotów obowiązanych leży dokonanie indywidualnej oceny z uwagi na właściwości klienta i inne okoliczności. Kryterium oceny może być bardzo różne, np. wynikać może ono z rodzaju przedmiotu lub usługi obrotu gospodarczego czy też charakterystycznych jego cech. Środki bezpieczeństwa podejmowane mają być stosownie do sklasyfikowanego ryzyka art. 33 ust. 4 u.p.p.p. Podmioty obowiązane muszą zatem wprowadzać odpowiednie procedury kwalifikacyjne ryzyko i w tym zakresie stosownie dobierać środki bezpieczeństwa wobec zagrożenia.

Środki bezpieczeństwa finansowego stanowi zakres art. 34 u.p.p.p. Wymóg w zakresie identyfikacji beneficjenta rzeczywistego klienta jest bezwzględny i odnosi się zarówno do osób prawnych, jak i fizycznych, a także jednostek organizacyjnych nieposiadających osobowości prawnej. Oprócz stałego elementu identyfikacji podmioty obowiązane są do uzasadnionych czynności, celem weryfikacji jego tożsamości, kontroli struktury własności i innych kontroli. Wymagane jest dokonanie oceny stosunku gospodarczego i wnikliwe monitorowanie stosunków

[40] *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Wolters Kluwer, Warszawa 2020, s. 225–227.

[41] Sprawozdanie Głównego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2020 r., Warszawa 2021, s. 35.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

o charakterze gospodarczym z klientem art. 34 ust. 4 u.p.p.p. Ponadto ustawodawca w art. 35 u.p.p.p. zawarł katalog przypadków, co do których obowiązkowo instytucje obowiązane mają stosować środki bezpieczeństwa finansowego. Wśród nich wymienić można samo nawiązanie stosunku gospodarczego, transakcje okazjonalne o wartości 15 000 euro lub wyższej, transakcje okazjonalne o wartości 10 000 euro lub wyższej, a także samo podejrzenie prania pieniędzy i finansowania terroryzmu czy wątpliwości w zakresie danych klienta. W zakresie środków bezpieczeństwa finansowego instytucje obowiązane z mocy ustawy uprawnione są do ich stosowania w modelu uproszczonym lub wzmożonym, w zależności od dokonanej przez nie oceny ryzyka związanego z klientem art. 43 i 44 u.p.p.p. Możliwe jest powierzenie stosowania środków bezpieczeństwa finansowego innemu podmiotowi art. 48 u.p.p.p. Od momentu zakończenia współpracy z klientem instytucje obowiązane są do archiwizowania przez okres 5 lat dokumentacji z klientem, potwierdzeń transakcji, wyników analiz. Dokumentacja ta może być na żądanie GIIF przechowywana przez okres kolejnych 5 lat, celem zapewnienia prawidłowego biegu prowadzonych postępowań związanych z praniem pieniędzy i finansowaniem terroryzmu art. 48, 49 u.p.p.p. Wymogiem w zakresie środków bezpieczeństwa jest wdrożenie procedur wewnętrznych dotyczących prania pieniędzy i finansowania terroryzmu i zapewnienia pracownikom udziału w programach szkoleniowych w zakresie wykonywania obowiązków związanych z praniem pieniędzy i finansowaniem terroryzmu. Stosownie do art. 50 u.p.p.p. instytucje obowiązane wdrażają wewnętrzne procedury w obszarze przeciwdziałania AML/CFT określającej stosowne zasady działania szczególnie w stosunku do katalogu otwartego art. 50 pkt. 2 u.p.p.p. Niewypełnienie obowiązku w zakresie zapewnienia funkcjonowania procedur wewnętrznych, w drodze których stosowane są środki bezpieczeństwa finansowego, stanowi naruszenie art. 8b u.p.p.p. Stosowanie środków bezpieczeństwa finansowego w odniesieniu do faktoringu i dokonywanego badania ryzyka faktoringowego nie stanowi analizy z uwagi na ryzyko prania pieniędzy. Rozróżnienia wymaga obowiązek badania ryzyka prania pieniędzy od dokonywanych innych badań ryzyka, jak w przypadku ryzyka faktoringowego dokonywanego w kontekście prowadzonej działalności gospodarczej[42].

Zgodnie z art. 30 ust. 3 dyrektywy AML państwa członkowskie obowiązane są do udostępniania aktualnych i szczegółowych informacji o beneficjentach rzeczywistych, czego odzwierciedleniem jest art. 55 u.p.p.p. ustanawiający Centralny Rejestr Beneficjentów Rzeczywistych CRBR, którego organem właściwym w jego sprawach jest MF[43]. Dane w rejestrze obejmują osoby fizyczne, do których kompetencji należy kontrolowanie w sposób pośredni lub bezpośredni spółki. Celem reje-

[42] VI SA/Wa 2645/13, Stosowanie środków bezpieczeństwa finansowego. Działanie przedsiębiorstw faktoringowych, Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie.

[43] *Instrukcje księgowe i podatkowe*, wyd. 2, red. A. Hołda, C.H. Beck, Warszawa 2020, s. 1325–1327.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

stru CRBR jest zwalczanie prania pieniędzy i finansowania terroryzmu. Ewidencja w rejestrze pozwala w sposób bezpośredni na ustalenie tożsamości osoby odpowiedzialnej w strukturze podmiotu obrotu gospodarczego[44]. Szczegółowy zakres podmiotowy beneficjentów określają ich definicje zawarte w art. 2 u.p.p.p. Odnoszą się one do osób fizycznych, trustów, a także określają zakres w stosunku do osoby prawnej innej niż spółka. CRBR stanowi transpozycję przepisów UE, której dokonano w ustawodawstwie krajowym w sposób rozszerzający. Szczegółowe zasady zgłaszania podmiotów do rejestru CRBR, wymogi w zakresie wniosku o wpis do rejestru, a także kwestie udostępniania informacji zostały unormowane w rozporządzeniu Ministra Finansów[45]. Dane zamieszczone w rejestrze są jawne, stosownie do przepisów dyrektywy AMLV w zakresie gwarancji standardów dostępu do informacji, także w zakresie rozszerzającym, tj. wszelkich zainteresowanych w tym także potencjalnych klientów i kontrahentów. Treść wpisu do rejestru objęta jest zasadą domniemania jego prawdziwości art. 68 u.p.p.p.[46], a także osoba zgłaszająca ponosi odpowiedzialność za szkodę wyrządzoną zgłoszeniem. W zakresie uchybienia obowiązkom związanym ze zgłoszeniem do CRBR zastosowana może być kara administracyjna w kwocie do 1 000 000 zł.

Obowiązane instytucje gromadzą i przekazują informacje GIIF. Obowiązki te wynikają z art. 72 i n. u.p.p.p. Wspomnieć należy jednak, iż obowiązkiem objęte są wpłaty i wypłaty transferów powyżej 15 000 euro. Obowiązek ten dotyczy także transferów środków pieniężnych zza granicy Rzeczypospolitej Polskiej. Instytucje obowiązane zobligowane są do niezwłocznego zgłoszenia GIIF okoliczności, co do których istnieje podejrzenie przestępstwa. Niezwłoczne przekazanie wymaganych informacji i dokumentów do GIIF następuje także w drodze każdorazowego żądania w tym zakresie. Zgodnie z art. 80 u.p.p.p. GIIF odbiera zgłoszenia o rzeczywistych i potencjalnych naruszeniach przepisów ustawy u przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Szczegółowy sposób odbierania zgłoszeń przez GIIF określa rozporządzenie[47]. W ramach współpracy krajowej prokurator zawiadamia GIIF w przypadku postanowienia o zablokowaniu rachunku, wstrzymaniu transakcji, wszczęciu postępowania, przedstawieniu zarzutów, a także w przypadku wniesienia aktu oskarżenia tytułem prania pieniędzy lub finansowania terroryzmu. Inne organy ścigania, w zakresie

[44] Serwis Rzeczypospolitej Polskiej Ministerstwa Finansów, https://www.gov.pl/web/finanse/centralny-rejestr-beneficjentow-rzeczywistych (data dostępu: 19 sierpnia 2021).

[45] Rozporządzenie Ministra Finansów z dnia 16 maja 2018 r. w sprawie wniosków o udostępnienie informacji o beneficjentach rzeczywistych oraz udostępniania tych informacji (Dz.U. z 2018 r., poz. 965).

[46] Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r., poz. 815).

[47] Rozporządzenie Ministra Finansów z dnia 16 maja 2018 r. w sprawie odbierania zgłoszeń naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 959).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wszczętych postępowań karnych dokonują zgłoszeń, stosownie do art. 83 u.p.p.p.[48]. W 2020 r. na podstawie art. 81 u.p.p.p. do GIIF wpłynęło 236 zawiadomień, co stanowi wzrost w odniesieniu od 2019 r. o 48 przypadków. Ustawowy termin na poinformowanie GIIF wynosi do 7 dni, przy czym przekazanie informacji powinno nastąpić niezwłocznie. Obowiązek niezwłocznego informowania prokuratury odnosi się również do GIIF w odniesieniu od informacji przekazanych przez prokuratora w związku czynem z art. 299 k.k.

Zawiadomienie GIIF przez instytucję obowiązaną o uzasadnionym podejrzeniu popełnienia przestępstwa w zw. z przedmiotową ustawą uprawnia organ do żądania wstrzymania transakcji lub dokonania blokady rachunku na okres nie dłuższy niż 96 godzin, art. 86 ust. 5 u.p.p.p., art. 87 u.p.p.p. a w przypadku uznania, iż może mieć to związek z przestępstwem. GIIF niezwłocznie powiadamia prokuratora o podejrzeniu popełnienia przestępstwa. Prokurator uprawniony jest do wydania postanowienia w przedmiocie wstrzymania transakcji i zablokowania rachunku na okres do 6 miesięcy art. 86 ust. 8 i 9 u.p.p.p.[49]. W przedmiocie żądania blokady GIIF zawiadamia również szefa ABW[50]. W zakresie nieuregulowanym ustawą do kwestii związanych z wstrzymywaniem transakcji i blokowania rachunków stosuje się odpowiednio ustawę Kodeks Postępowania Karnego, art. 98 u.p.p.p.[51].

Instytucje obowiązane na podstawie art. 177 u.p.p.p. uprawnione są w do stosowania szczególnych środków ograniczających, do których należy możliwość zamrożenia wartości majątkowych i blokada przeprowadzania na nich operacji i obrót nimi, a także nieudostępnianie wartości majątkowych. Zakres podmiotowy zgodnie z art. 118 u.p.p.p. obejmuje osoby fizyczne i inne podmioty wykazane na listach publikowanych przez GIIF na podstawie rezolucji Rady Bezpieczeństwa ONZ w związku z postanowieniami Karty Narodów Zjednoczonych o zagrożeniach pokoju i bezpieczeństwa. Stosowanie szczególnych środków ograniczających odbywa się bez uprzedniego informowania, a informacje o dokonanych blokadach przekazywane są zgodnie z art. 119 u.p.p.p.[52] do GIIF. Listę osób i podmiotów, w zakresie których przepisy o szczególnych środkach ograniczających mają zastosowanie prowadzi GIIF, który także wydaje decyzję o wpisie na listę, której podstawą jest rekomendacja KBF. Brak regulacji z uwagi na dyspozycję art. 75

[48] P. Walczak, *Dokumentacja wewnętrzna w jednostkach sektora finansów publicznych*, C.H. Beck, Warszawa 2020, s. 230–233.

[49] M. Kędzierski, *Obowiązki i odpowiedzialność oficera AML (AMLO) w instytucji obowiązanej (cz. 1.)*, „Prokuratura i Prawo" 2021, nr 5, s. 78–80.

[50] M.A. Kędzierski, *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Przegląd Bezpieczeństwa Wewnętrznego, Agencja Bezpieczeństwa Wewnętrznego" 2020, s. 120–143.

[51] Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r., poz. 815).

[52] *Ibidem*.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

TFUE[53] w drodze zakreślenia przez UE ram środków administracyjnych stosowanie szczególnych środków ograniczających może dotyczyć również podmiotów zagranicznych. Do decyzji wydawanych w zakresie wpisu na listę zastosowanie znajdują przepisy kodeksu postępowania administracyjnego[54]. Osoby fizyczne będące beneficjentami rzeczywistymi lub wspólnikami którejś z działalności wymienionych w art. 2 ust. 1 pkt 16 i 18 u.p.p.p. spełniać muszą wymóg niekaralności za umyśle przestępstwo lub przestępstwo skarbowe.

Instytucje obowiązane, które nie dopełniły nałożonych na nie wymagań wyszczególnionych w art. 147 – 149 u.p.p.p., popełniają w rozumieniu prawa administracyjnego delikt i z tego tytułu podlegają karze administracyjnej. Szczegółowy katalog kar zawarty został w art. 150 u.p.p.p., gdzie najważniejsze to publikacja informacji o podmiocie, zakaz podejmowania czynności, zakaz zajmowania stanowiska kierowniczego i kary pieniężne. W stosunku do osób fizycznych kara pieniężna nałożona może sięgnąć maksymalnie wartości 20 868 500 zł, a w przypadku osób prawnych i jednostek nieposiadających osobowości prawnej do wartości 5 000 000 euro. Organami uprawnionymi na podstawie art. 151 u.p.p.p. do nakładania kar administracyjnych są GIIF, prezes NBP, KNF, MF. Decyzje w zakresie nałożonych kar administracyjnych podawane są do publicznej wiadomości poprzez zamieszczenie ich treści w BIP Ministerstwa Finansów.

Ustawa zawiera także przepisy karne. W zakresie niedopełnienia obowiązków przekazania GIIF zgłoszenia o podejrzeniu popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, czy też zgłoszenia słusznie uzasadnionego podejrzenia, że przedmiot transakcji może mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, czyli w zw. z art. 76 i 86 u.p.p.p. podlega sankcji karnej w wymiarze od 3 miesięcy do 5 lat pozbawienia wolności. Taką karą obwarowane jest także udzielenie nieprawdziwych informacji i zatajenie informacji. Karze tej podlega także ujawnienie nieuprawnionemu informacji zgromadzonych zgodnie z ustawą. Karze grzywny podlega osoba, jeżeli działała w sposób nieumyślny. Odpowiedzialność karana w zakresie art. 156 u.p.p.p. dotyczy jedynie osób fizycznych pełniących obowiązki na rzecz instytucji obowiązanej lub ją reprezentujących czy też upoważnionych do zaciągania zobowiązań w jej imieniu. Należy przez to rozumieć w pierwszej kolejności osoby upoważnione w myśl art. 7 i 8 u.p.p.p.[55].

[53] Traktat o Unii Europejskiej i Traktat o funkcjonowaniu Unii Europejskiej, Dziennik Urzędowy C 326, 26/10/2012 P. 0001 – 0390.

[54] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 1960 r., nr 30, poz. 168).

[55] Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r., poz. 815).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

6.4. GLOBALNE ZAGROŻENIA I WYZWANIA REGULACJI W OBSZARZE SEKTORA FINTECH I FUNKCJONOWANIA OBOWIĄZANYCH INSTYTUCJI FINANSOWYCH

Realizacja zwalczania zjawiska prania pieniędzy i finansowania terroryzmu odbywa się przy współpracy międzynarodowej, dzięki czemu efektywność działań znacząco się zwiększa. Globalne zjawisko przestępczości zorganizowanej prania pieniędzy i finansowania terroryzmu wymaga zorganizowanych międzynarodowo globalnych reakcji organów ścigania[56]. Do najważniejszych Instytucji Międzynarodowych w walce z praniem pieniędzy i finansowaniem terroryzmu można zaliczyć:

- BCBS – Basel Committee on Banking Supervision – Bazylejski Komitet ds. Nadzoru Bankowego powołany w 1974 r. przez banki centralne państw grupy G10. Komitet wydał liczne deklaracje i zalecenia oraz tzw. dobre praktyki, wypracowane standardy uwzględniono w Dyrektywie AML. Jako pierwszy wypracował KYC – *know your costomer*,
- ONZ – Organizacja Narodów Zjednoczonych, której dorobkiem jest szereg konwencji, w tym także o przedmiocie przestępczości zorganizowanej i zwalczaniu obrotu środkami psychotropowymi. W drodze ratyfikacji przez państwa sygnatariuszy staje się prawem krajowym po jej ogłoszeniu w D.U.Rzeczypospolitej Polskiej art. 91 Konstytucji RP[57],
- FATTF (Financial Action Task Force) jest międzynarodową organizacją rządową o charakterze specjalnym do przeciwdziałania praniu pieniędzy. Utworzona w 1989 opracowuje i wdraża standardy międzynarodowe. Publikuje także raporty o zagrożeniach związanych z procederem. Wypracowuje wolę polityczną do przeprowadzenia reform legislacyjnych, celem wdrożenia przepisów. Udziela wsparcia państwom w zakresie wdrażania przepisów AML/CFT[58],
- MONEYVAL – jest stałym organem monitorującym Rady Europy o charakterze kontrolnym. Zadaniem organu jest ocena zgodności wdrażania i realizowania standardów, zaleceń przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Organ ten wydaje również niezbędne zalecenia władzom krajowym. Zgodnie z podpisanym statutem organ ten jest niezależnym organem moni-

[56] M. Smolak, *formy zwalczania procedur prania pieniędzy*, „Przegląd Bezpieczeństwa Wewnętrznego" 9/13, s. 301–302.

[57] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483).

[58] Portal internetowy FATF, https://www.fatf-gafi.org/about/.(data dostępu: 22 sierpnia 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

torującym podległym bezpośrednio Komitetowi Ministrów[59]. W maju 2021 r. ewaluatorzy Komitetu MONEYVAL Rady Europy odbyli w Rzeczypospolitej Polskiej wizytację, celem oceny naszego systemu prawnego w zakresie AML/CFT. Ostatnia wizytacja miała miejsce 9 lat temu, czyli 2012 r.[60],

- EGMONT Group – Międzynarodowa organizacja, w ramach której funkcjonuje 167 jednostek analityki finansowej. Zapewnia ona platformę do wymiany informacji w zakresie wywiadu finansowego celem ułatwienia globalnego zwalczania prania pieniędzy i finansowania terroryzmu. Jednostki analityki (FIU) na podstawie standardów międzynarodowych AML/CFT obowiązane są do wymiany informacji[61].

Funkcjonujący sektor FinTech wyróżnia się także z uwagi na technologie regulacyjne tzw. RegTech – Regulatory Technology. Sektor ten zajmuje się regulacjami technologicznymi i jest jednym z najdynamiczniej rozwijających się sektorów w przedmiocie innowacji. W ramach funkcjonowania tego sektora funkcjonują firmy zajmujące się opracowaniem i wprowadzaniem technologii i metod, a także zastosowaniem rozwiązań mających na celu dostosowania w zakresie wymogów ustawodawcy. Sektor RegTech wykorzystując nowe technologie ułatwia lub też w pełni rozwiązuje problemy spełnienia wymogów ustawodawcy nałożone na podmioty obrotu gospodarczego, takie jak np. kryteria nadzorcze, kontrolne, dokumentacji, standardów. Procesy wykorzystywane w RegTech to głównie aktualizacja procesów informatycznych, oprogramowania, metod analitycznych, a także procedur zarządczych w instytucjach finansowych sektora FinTech. Przedmiotem aktualizacji RegTech są m in. procesy identyfikacji i zarządzania ryzykiem, zarządzanie kontrolą, analiza rynku, technologia monitoringu transakcji płatniczych, trending finansowy[62].

Kolejną innowacją w sektorze FinTech i RegTech jest branża SubTech – Supervisior Technology. W ramach sektora SupTech wyspecjalizowane do tego firmy zajmują się gromadzeniem analizą i kompilacją danych, także z wykorzystaniem chmury obliczeniowej. Zapotrzebowanie na tę branżę zachodzi w obowiązkach nadzorczych i kontrolnych, raportowaniu nieprawidłowości. Dostęp do szczegółowych danych o każdej transakcji następuje w sposób szybki, przystępny i uporządkowany, a przede wszystkim oszczędny dla przedsiębiorcy, który wybrał zastosowanie tej metody rozwiązania. SupTech jest także technologiczną metodą nadzoru

[59] Resolution CM/Res(2013)13 on the statute of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) (Adopted by the Committee of Ministers on 9 October 2013 at the 1180th meeting of the Ministers' Deputies).

[60] gov.pl, https://www.gov.pl/web/finanse/wizyta-ekspertow-komitetu-moneyval-rady-europy (data dostępu: 22 sierpnia 2021).

[61] Egmont Group, https://www.egmontgroup.org/en/content/about (data dostępu: 22 sierpnia 2021).

[62] M. Folwarski, *Sektor FinTech na Europejskim Rynku Usług Bankowych*, Poltex, Warszawa 2019, s. 73–87.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

w rękach podmiotów nadzorczych usprawniając podejmowane przez nie działania. Sektor SupTech w zakresie analizy danych dokonuje przygotowania danych na potrzeby wymogów AML/CFT, ryzyka związanego z oszustwami, transakcji niewiadomego pochodzenia. Obszar ten obejmuje także analizę makroostrożnościową i mikroostrożnościową. Wyspecjalizowane możliwości, jakimi posługuje się sektor SupTech, pozwalają nie tylko na sprawne gromadzenie i przetwarzanie danych, ale dostęp do nich w czasie rzeczywistym. Ponadto oferowane są narzędzia, statystyki, raporty, podgląd rzeczywisty, podgląd historyczny. Firmy specjalizujące się w branży SupTech wyspecjalizowane są w gromadzeniu i analizie danych[63].

Z perspektywy globalnej należy podkreślić jeszcze funkcjonowanie sektora BigTech. Firmy tego sektora to giganty na rynku informatycznym wykorzystujące nowoczesne technologie do m.in. eksploracji, klasyfikacji i zobrazowania klienteli. Dzięki tym analizom dokonywana jest zmiana dostarczanych usług i sprzedaży produktów dostosowanych do potrzeb, jak również kreacja modeli biznesowych, dzięki którym odbywa się ta dystrybucja produktów i usług. Niewątpliwie wobec tak skonstruowanych instrumentów finansowych funkcjonowanie tradycyjnych banków czy nawet ich modeli międzynarodowych będzie musiało podjąć konkurencję w oparciu o podobne rozwiązania. Możliwe jest również podjęcie tych starań w oparciu o całkiem nowe rozwiązania biznesowe wpisujące się w nowoczesny ekosystem funkcjonowania usług i dostarczania produktów. Do sektora BigTech możemy zaliczyć podmioty takie, jak: Google, Facebook, Twitter, Amazon, Allegro[64].

Rozwój sektora FinTech wpłynął ogromnie na bankowość indywidualną, przez co dokonała się cyfryzacja usług bankowych z wykorzystaniem nowych modeli biznesowych. W celu utrzymaniu klienteli na rynku banki zaczęły zmieniać zakres swoich usług, aby utrzymać klientów. W tym miejscu należy jednak odróżnić banki od tradycyjnych FinTechów, pomimo iż mogą one oferować podobne do siebie usługi np. kredyty czy prowadzenie rachunku konta walutowego[65].

Modele biznesowe wykorzystywane w sektorze FinTech skoncentrowane są wokół funkcjonalności i dostępności technologii i możliwościach jej wykorzystania. Model oparty na płatnościach udostępnia możliwość wykorzystania P2P, płatności bezgotówkowych i mobilnych w czasie rzeczywistym. Jest więc szybkim powszechnym modelem biznesowym, w którym transakcje rozliczane są na

[63] *Ibidem,* s. 73–85.

[64] M. Sawicki, *Wpływ pandemii (Covid-19) na zamianę modeli biznesowych na przykładzie branży bankowej w Polsce*, Zeszyty Naukowe ZPSB, Firma i Rynek 2021, nr 1 (59), s. 27–38.

[65] A. Fierla red., P. Dec (w:) *Wokół finansjeryzacji. Wybrane zagadnienia*, Rozdział III: *Rozwój sektora FinTech a tradycyjna bankowość – ujęcie ilościowe*, Oficyna Wydawnicza SGH, Warszawa 2018, s. 51–65.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

bieżąco. Wykorzystanie tego modelu znajduje zastosowanie przeważnie w branży detalicznej[66].

Wykorzystanie modelu zarządzania majątkiem w FinTech polega na automatyzacji świadczonych usług finansowych przy pomocy robo-doradztwa. Model ten wykorzystywany jest na rynku kapitałowym, w handlu algorytmicznym, wykorzystaniem robo-doradztwa, czyli zautomatyzowanego doradztwa w zakresie instrumentów inwestycyjnych[67]. Robo-doradztwo zostało przez UKNF dostrzeżone jako narzędzie dla rozwoju rynku inwestycyjnego wpisując się w plan działania Cyfrowej Agendy Nadzoru KNF[68].

Model biznesowy w postaci crowdfundingu polega na cyfrowym finansowaniu przez ludzi różnych celów. Mogą to być projekty biznesowe, obyczajowe, powiązane ze sztuką i kulturą. Jest to zatem finansowanie społecznościowe. Gromadzenie środków pieniężnych polega na zasadzie dobrowolnych, nawet bardzo drobnych wpłat. Oddziaływanie społeczne w postaci, pomysłu na oryginalny biznes, chęci uzyskania pomocy, wyjścia z nowym pomysłem kreatywnym, któremu przyświeca cel zbiórki finansowej może być realizowany tylko za pośrednictwem sieci IT i tylko w formie gotówkowej. Z uwagi na te uwarunkowania model biznesowego FinTech świetnie wpisuje się crowdfunding[69].

Model pożyczkowego FinTecha (*money lending*) z wykorzystanie P2P stanowi niezwykle przystępne narzędzie do udzielania pożyczek klienteli w tym także pożyczek waluty wirtualnej jak BTC-Bitcoin, i innych, czy także pożyczek biznesowych. Model ten jest konkurencyjny w stosunku do tradycyjnych instytucji finansowych jak np. banki[70].

Według raportu o stanie europejskiego FinTechu na 2021 r., opracowanego przez zespół Tech.eu zajmujący się opracowywaniem i publikowaniem stanu ekonomicznego systemu finansowo-technologicznego europejskie firmy FinTech zebrały w 2018 r. łącznie 3,52 mld USD. Natomiast w 2019 r. liczba ta wzrosła o 150% do 8,81 mld USD. Przykładowo we wrześniu 2020 r. firma Klarna zebrała 650 mld USD, a jej wycena sięgnęła 10,65 bln USD. W styczniu 2021 r. firma Checkout.com osiągnęła wycenę na 15 bln USD, po doinwestowaniu jej o kwotę

[66] FinTech, a*Płatności odroczone, rozwój e-commerce i usługi chmurowe. Rok pandemii w sektorze FinTech*, https://fintek.pl/platnosci-odroczone-rozwoj-e-commerce-i-uslugi-chmurowe-rok-pandemii-w-sektorze-fintech (data dostępu: 21 sierpnia 2021).

[67] M. Nowakowski, *op. cit*., s. 238–245.

[68] Publikacja Komisji Nadzoru Finansowego „Cyfrowa Agenda Nadzoru" – plan działań Urzędu KNF w zakresie m.in. nowoczesnych technologii, innowacji oraz cyberbezpieczeństwa, Warszawa 2019.

[69] K. Kozioł-Nadolna, *Crowdfunding jako źródło finansowania innowacyjnych projektów,* Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubezpieczenia, nr 73, Szczecin 2015, s. 671–683.

[70] K. Kocoń, *Prawnopodatkowe aspekty pozyskiwania kapitału w ramach finasowania społecznościowego przez mikro i małe przedsiębiorstwa*, „Finanse, Rynki Finansowe, Ubezpieczenia" 2017, nr 4 (88), cz. 2, s. 207–2011.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

450 mln USD. W lipcu 2020 r. TransferWise osiągnął wycenę 5 mld USD. Zgodnie z raportem do 5 największych FinTechów w Europie należy zaliczyć Klarna, Lendify, Monzo, OakNorth, Revolut[71].

W sektorze FinTech rozpowszechnione jest funkcjonowanie w oparciu o odpowiednie licencje transgraniczne tzw. NeoBanków. Usługi świadczone przez neobanki odbywają się w pełni przy pomocy sieci internetowej. Wykorzystują one technologie finansowe i dedykowane są głównie dla klientów, którzy dobrze czują się z nową technologią[72]. Dostęp uzyskuje się w zasadzie zaraz po zainstalowaniu aplikacji i rejestracji konta w systemie. Należy zaznaczyć iż neobanki są zupełnie czymś innym niż tradycyjne banki, ponieważ w zależności do rodzaju i zakresu licencji nie oferują wszystkich usług, jakie mogą oferować banki tradycyjne. Przyjmowane są także rozwiązania polegające na usłudze połączonej, w której tradycyjny bank połączony jest z neobankiem. Klienci neobanków ponoszą niższe koszty, ponieważ podmioty te nie ponoszą ryzyka kredytowego, a unormowanie ich działalności występuje w mniejszym zakresie niż w stosunku do tradycyjnych banków. Indywidualizują się sprawnym szybkim przetwarzaniem danych, przez wykorzystanie wysoce wyspecjalizowanej technologii informatycznej. Dzięki temu klienci mogą załatwić sprawę szybciej, bez konieczności odbywania długich procedur, przyspieszając w ten sposób procesy, np. w przypadku pożyczek system jest w stanie zakwalifikować pożyczkobiorcę w klika minut[73]. Ranking Top10MobileBanks podaje, iż na sierpień 2021 r. do 5 największych neobanków w Europie należą N26, Soldo, Bunq, Wise, Ferratum Bank[74].

Poddając ocenie ryzyko związane z funkcjonowaniem sektora FinTech należy zwrócić uwagę, iż sektor ten dotyczy także rynku walut wirtualnych. Rynek walut wirtualnych z uwagi na brak ustawy szczególnej jest rynkiem nieregulowanym. KNF wskazuje na liczne nieprawidłowości, które występują na rynku kryptowalut. W 30% wartość wyemitowanych produktów ICO – Initial Coin Offering (Tokenizacja) spadła do zera, a nieprawdziwe zbiórki szacuje się nawet w granicach 80%. Ryzyko powstaje również na skutek braku możliwości zabezpieczenia przed utratą środków w całości lub w części, a także z uwagi na nieznajomość aktywów i zasad ich funkcjonowania i niedostateczne rozeznanie w produktach, jakie są

[71] Raport of Tech.eu, The State-of-European-FinTech, January 2021, https://tech.eu/wp-content/uploads/woocommerce_uploads/2021/01/State-of-European-FinTech-0h4ee7.pdf (data dostępu: 21 sierpnia 2021).

[72] J. Górka, *Banki, GAFAM, FinTech w gospodarce współdzielenia – equilibrium współpracy i konkurencji*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 531, Wrocław 2018, s. 150–158.

[73] PortfelInternetowy.com, https://www.portfelinternetowy.com/neo-banki-dowiedz-sie-czy-sa-fintech-i-jakie-niosa-korzysci (data dostępu: 21 sierpnia 2021).

[74] Top10mobilebanks.com, https://top10mobilebanks.com/best-mobile-banks-dtop-t2/?edgetrackerid=100381575405706&gclid=CjwKCAjwyIKJBhBPEiwAu7zll2rVijTG3FsUWvUgRmWYdwRgyt8n1b1vYzIjMSOfuQWzjYfBfRPV3hoC_AQQAvD_BwE (data dostępu: 21 sierpnia 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

przedmiotem inwestycji[75]. W nawiązaniu do Rezolucji Parlamentu Europejskiego, w pkt. 5.1 podniesiono aspekt edukacyjny podkreślając, iż wiedza finansowa i umiejętności cyfrowe stanowią kluczowe elementy wpływające na wykorzystanie technologii finansowej i zmniejszenie ryzyka związanego z inwestycją, podkreślając w pkt. 5.2, iż edukacja konsumentów detalicznych jest konieczna, także dla niej samej, aby mogła stać się narzędziem i częścią obrotu gospodarczego[76]. Największymi zagrożeniami w obrocie walutami wirtualnymi, na które zwraca uwagę KNF, są piramidy finansowe Panziego i inne podobne systemy piramidowe, nielegalne zbiórki na określony rzekomo cel, dokonywanie inwestycji u podmiotów nieposiadających zezwoleń na prowadzenie działalności związanej z obrotem walutami wirtualnymi oferujących niekiedy instrumenty inwestycyjne bez wymaganych zezwoleń[77]. Liczne są także przypadki włamań hackerskich i kradzieży kryptoaktywów, a także oszustw w drodze nieuprawnionych podmiotów świadczących usługi obrotu walutami wirtualnymi[78].

Usługodawcy dążą do maksymalizacji środków zabezpieczenia i wyeliminowania zjawiska, jednakże całkowite wyeliminowanie zjawiska najprawdopodobniej nigdy w pełni nie nastąpi[79].

Wzrost cyfryzacji i rozwój technologii DLT/Blockchain wymaga zapotrzebowania dostosowania prawa w tym zakresie także na szczeblu Unii Europejskiej. Projekt zmian w tym przedmiocie stanowi Wniosek Rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniający dyrektywę (UE) 2019/1937[80]. Perspektywy wizji gospodarki cyfrowej wykorzystującej innowacje technologiczne na szeroką skalę, w tym także technologię rozproszonego rejestru DLT/Blockchain wymogły fakt, iż banki centralne rozpoczęły konfrontacje w perspektywie wykorzystania i zapewnienia funkcjonalności wykorzystania tej technologii. Departament Systemu Płatniczego Narodowego Banku Polskiego w maju 2021 r. opublikował opracowanie poświęcone cyfrowemu pieniądzu banku centralnego. Central Bank Digital Currency – CBDC jest to projekt emisji

[75] Pismo z dnia 12 stycznia 2021 r. Urząd Komisji Nadzoru Finansowego, Ostrzeżenie o ryzykach związanych z nabywaniem oraz z obrotem kryptoaktywami (w tym walutami wirtualnymi oraz kryptowalutami).

[76] Rezolucja Parlamentu Europejskiego z dnia 17 maja 2017 r. w sprawie FinTech: wpływ technologii na przyszłość sektora finansowego (2016/2243(INI)) (Dz.U. UE. C. z 2018 r., nr 307, s. 66).

[77] Pismo z dnia 12 stycznia 2021 r. Urząd Komisji Nadzoru Finansowego, Ostrzeżenie o ryzykach związanych z nabywaniem oraz z obrotem kryptoaktywami (w tym walutami wirtualnymi oraz kryptowalutami).

[78] P. Opitek, *Pranie, przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 50–52.

[79] Inwestopeia, *What are the Legal Risks to Cryptocurrency Investors?*, Nathan Reiff, Jun 25, 2019 r. https://www.investopedia.com/tech/what-are-legal-risks-cryptocurrency-investors/.

[80] Wniosek Rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/193, Bruksela, 24 września 2020, COM(2020) 593 final, 2020/0265(COD).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

pieniądza cyfrowego przez bank centralny. W dokumencie tym podkreślono, iż pomimo dużej popularności walut wirtualnych i technologii DLT/Blcokchain nie jest ona na tyle rozwinięta, a także bezpieczna, aby można było ją z powodzeniem wykorzystać do wprowadzenia jako trwałe rozwiązanie środka płatniczego[81].

6.5. PODSUMOWANIE

Rada Ministrów Rzeczypospolitej Polskiej podjęła 11 maja 2021 r. uchwałę w sprawie przyjęcia strategii przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Strategia opisuje plan działań i wytycza rekomendacje w odniesieniu do Krajowej Oceny Ryzyka prania pieniędzy oraz finansowania terroryzmu, która została opublikowana przez GIIF w 2019 r. Postanowienia Krajowej Oceny Ryzyka muszą zostać również uwzględniona przez instytucje obowiązane przy dokonywaniu przez nie oceny własnego ryzyka.

Zgodnie z Krajową Oceną Ryzyka z 2019 r. największy poziom prawdopodobieństwa wystąpienia ryzyka stanowią[82]:

- nielegalny przewóz wartości majątkowych przez granicę, przez osoby fizyczne,
- wymiana waluty,
- legitymowanie nielegalnych środków w drodze działalności gospodarczej podmiotów trzecich,
- wykorzystywanie usług telekomunikacji o podwyższonej płatności do legitymowania środków,
- crowdfunding,
- wykorzystanie internetowych usług płatniczych do transferów nielegalnych środków,
- wykorzystywanie obrotu walut wirtualnych,
- pranie pieniędzy z wykorzystywaniem organizacji typu non-profit, np. fundacji, stowarzyszeń,
- pranie pieniędzy z wykorzystaniem obrotu dobrami o wysokiej wartości, złota, kamieni szlachetnych,
- bankowość,
- hazard.

Krajowa Ocena Ryzyka będąca punktem odniesienia dla Krajowego Systemu Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu stanowi o zakresie strategii obejmujące 4 obszary. Legislacyjnym, w zakresie potrzeby regulacji praw-

[81] Publikacja Narodowego Banku Centralnego, Departament Systemu Płatniczego NBP Warszawa, maj 2021, Pieniądz cyfrowy Banku Centralnego.

[82] Krajowa Ocena Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu, Warszawa 2019.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nych, systemu edukacji w drodze szkoleń pracowników JAF, jednostek współpracujących i instytucji obowiązanych, wymiany informacji z wykorzystaniem internetu, a także skuteczniejsze gromadzenie i generowanie szczegółowych danych statystycznych. Koncepcje zmian w tym zakresie zakładają, iż KSPPFT opierać musi się o centrum wymiany informacji w jednostce JAF przynosząc efekt synergiczny dla całego systemu. Pracownicy organów ścigania mogą być delegowani do pracy w Departamencie Informacji Finansowej, Analizy GIIF powinny być zautomatyzowane, a wymiana informacji i dokonywanie zgłoszeń z udziałem instytucji obowiązanych w pełni zinformatyzowane. Postuluje się również analizę przepisów obowiązującego prawa pod kątem ograniczenia płatności gotówkowych do określonych limitów, celem ograniczenia anonimowego obrotu gotówkowego. Krajowa ocena ryzyka powinna zawierać środki łagodzące w odniesieniu od wskazanych ryzyk. Podmioty KSPPFT powinny dokonywać wymiany wiedzy i doświadczeń, zarówno przy użyciu środków teleinformatycznych, ale i w drodze szkoleń oraz e-learningu. Wymagane jest zapewnienie wsparcia KBF w postaci rady do spraw rozwiązań w zakresie nowych produktów. W zakresie swojej działalności rada współpracowałaby z instytucjami badawczymi, uczelniami wyższymi i innymi jednostkami. Ważnym punktem jest także wyposażenie każdego pomiotu KSPPFT w możliwość generowania informacji, danych statystycznych, wyliczeń, dokonywania ocen szacunkowych. Priorytetem rozwoju KSPPFT jest poprawa skuteczności działania JAF, dostosowanie instytucji obowiązanych w zakresie nowych zagrożeń, harmonizacja kontroli i nadzoru w systemie. Rozwój zakłada również optymalizację wymiany informacji i wprowadzenie jednolitych zasad generowania informacji[83].

Realizacja znamion czynu zabronionego nie musi stanowić spektakularnego przedsięwzięcia. Odbywać może się poprzez zainwestowanie środków pochodzących z czynu zabronionego w podmiot obrotu gospodarczego, który funkcjonuje w oparciu o kapitał pochodzenia legalnego. Proceder ten ma na celu uwierzytelnienie kapitału nielegalnego poprzez wprowadzenie go do obrotu jako legalnie wypracowany kapitał. Dla realizacji znamion czynu zabronionego nie jest wymagane w pełni „wypranie" kapitału, czyli realizacji wszystkich etapów mających na celu wprowadzenie nielegalnie pozyskanych środków do systemu finansowego. Kryminalizowany jest każdy z etapów mechanizmu mającego na celu stworzenie pozorów legalnego pochodzenia środków pochodzących z czynu zabronionego[84].

Zarówno ryzyko operacyjne, którego podmiotem są procedury wewnętrzne i systemy zarządcze, ryzyko finansowe i inwestycyjne, jak i funkcjonowanie instytucji obowiązanych oparte jest o możliwości adaptacyjne. Dostosowanie

[83] Uchwała nr 50 Rady Ministrów z dnia 19 kwietnia 2021 r. w sprawie przyjęcia strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (M.P. z 2021 r., poz. 435).

[84] II AKa 289/17, Czynności stanowiące pranie pieniędzy – Wyrok Sądu Apelacyjnego w Warszawie.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

się w zakresie wymogów prawnych, jak i zmieniającego się ryzyka i warunków rynku finansowego. Kluczowe znaczenie w przedmiocie walki z szeroko pojmowanym procederem prania pieniędzy wykorzystującym nowe innowacyjne technologie skutecznie postępować musi przy współpracy instytucji międzynarodowych i współpracy krajów, wyspecjalizowanych w walce ze zorganizowaną przestępczością finansową[85].

Przeciwdziałanie praniu pieniędzy jest stosunkowo nowym przedsięwzięciem, w odpowiedzi na nową zorganizowaną przestępczość finansową. Niemniej w płaszczyźnie globalnej problematyka oddziaływa na międzynarodowy system finansowy. Swoboda gospodarcza i swobodny przepływ usług i kapitału wykorzystywane są jako narzędzie pośrednie do maskowania środków finansowych przy użyciu różnego rodzaju nowinek technologicznych i instrumentów finansowych, zasadnym zatem jest ograniczanie na szeroką skalę możliwości anonimowego wykorzystywania instytucji finansowych do niewiadomych i skomplikowanych transferów[86].

[85] M. Capiga, *Bezpieczeństwo instytucji finansowych jako instytucji obowiązanych w systemie przeciwdziałania praniu pieniędzy*, Studia Ekonomiczne, Zarządzanie instytucjami finansowymi w niestabilnym otoczeniu gospodarczym, Uniwersytet Ekonomiczny w Katowicach nr 171, Katowice 2014, s. 120–131.

[86] P. Siejczuk, *Problematyka prania brudnych pieniędzy w regulacjach prawnomiędzynarodowych, europejskich i krajowych,* „Bezpieczeństwo Narodowe" 2012, nr III–IV, s. 220–223.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Adam Życzkowski
Wyższa Szkoła Gospodarki Euroregionalnej
w Józefowie

ROZDZIAŁ 7.

ROZWÓJ ZAUTOMATYZOWANYCH TECHNOLOGII WSPIERAJĄCYCH AML I CFT

7.1. UWAGI WPROWADZAJĄCE

Celem niniejszego rozdziału jest dokonanie analizy technologii wspierających AML i CFT oraz ustalanie potrzeb i zakresu wsparcia, jakimi dostępne na rynku narzędzia powinny się charakteryzować, aby sprostać wyzwaniom nakładanym na sektor finansowy przez dynamiczną zmianę wynikającą z jego cyfryzacji.

Założenia badawcze koncentrują się również wokół zmian prawnych, dotyczących rozwoju cyfrowego na poziomie europejskim i krajowym (część 2), autor dokonuje także analizy w kontekście głównych trendów w innowacjach cyfrowych oraz ich wpływu na ryzyka związane z AML i CFT (część 3). Niniejszy rozdział opisuje strategiczne cele europejskich finansów cyfrowych (część 4). Opisane zostały również cztery priorytety i powiązane działania, które Parlament Europejski podejmuje, aby umożliwić konsumentom i przedsiębiorstwom czerpanie korzyści z technologii cyfrowych finansów, przy jednoczesnym ograniczeniu ryzyka (część 5). Rozdział ten opiera się na pracach europejskiego regulatora w zakresie technologii finansowych z 2018 r.[1] (i lat późniejszych), który to opracował plan działania w pełnym zakresie. Aby uzupełnić wnioskowanie dotyczące wpływu nowoczesnych technologii na sektor finansowy dokonano przeglądu dostępnych narzędzi oraz prześledzono wyzwania związane z cyfryzacją, AML i ochroną danych (część 6, 7, 8). Rozdział podsumowuje krótka analiza porównawcza sztucznej inteligencji i potencjału, jaki ta technologia daje sektorowi finansowemu.

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Plan działania w zakresie technologii finansowej", COM(2018) 109 Final, 8 marca 2020.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Na koniec I kwartału 2021 r. na rynku polskim znajdowało się 44,115 mln kart płatniczych, to jest więcej o 441 tys. kart niż na koniec 2020 r. (wzrost o 1%). W Polsce na koniec marca 2021 r. było 38,9 mln szt. kart zbliżeniowych. Na przestrzeni I kwartału 2021 r. liczba takich kart zwiększyła się o 574 tys. szt. Udział kart zbliżeniowych w ogólnej liczbie kart płatniczych wyniósł 88,3% (w poprzednim kwartale stanowił on 87,8%)[2].

W I kwartale 2021 r. wolumen transakcji z wykorzystaniem kart płatniczych przekroczył 1,644 mld (transakcji gotówkowych oraz bezgotówkowych) na łączną kwotę 198,2 mld zł[3].

Jednocześnie biorąc pod uwagę omawiany okres udział wartości transakcji bezgotówkowych w ogólnej wartości transakcji przeprowadzonych przy użyciu kart płatniczych wyniósł 51,5%. Na przestrzeni ostatniego roku wskaźnik ten zwiększył się o 3,6 punktu procentowego.

Badania opublikowane przez izbę płatności cyfrowych pokazują, że najpopularniejszymi narzędziami płatniczymi są:

- karty płatnicze,
- rachunki bankowe z dostępem online do rachunku,
- konto bankowe bez aktywnego dostępu przez Internet.

Na pierwszym miejscu z wynikiem 47% jest karta płatnicza – w tym przypadku porównując do 2019 r. nie zaszła żadna zmiana. Na drugim miejscu jest konto bankowe z aktywnym dostępem przez Internet. 40% Polaków posiada takie konto. Oba instrumenty zatem stanowią trzon. Trzecie miejsce zajmuje konto bankowe bez aktywnego dostępu przez Internet (25%) – w tym przypadku nastąpiła zmiana w rankingu. W 2019 r. ankietowani wskazywali na konto w serwisie PayPal, które w 2020 r. spada na piątą pozycję[4].

Jednocześnie warto zauważyć, że na czwartym miejscu pojawiły się aplikacje mobilne banków, które umożliwiają dokonywanie płatności. Chodzi przede wszystkim o dwa modele płatności mobilnych – płatności BLIK oraz płatności HCE, czyli płatności zbliżeniowe telefonem. Używanie tego typu produktu deklaruje niemal jedna czwarta ankietowanych (23%). Ankietowani deklarują również używanie licznych aplikacji mobilnych, umożliwiających płatności (np. SkyCash, mPay, moBILET, Twisto, Revolut, N26).

Należy zgodzić się z poglądem, że cyfryzacja to przyszłość finansów: konsumenci i przedsiębiorstwa coraz częściej uzyskują dostęp do usług finansowych w sposób cyfrowy. Innowacyjni uczestnicy rynku wprowadzają nowe technologie, a istniejące modele biznesowe ewoluują w kierunku nowoczesnych rozwiązań tech-

[2] Narodowy Bank Polski, System płatniczy, https://www.nbp.pl/home.aspx?f=/systemplatniczy/karty_platnicze.html, s. 1 (data dostępu: 16 sierpnia 2021).

[3] *Ibidem*, s. 12, 14.

[4] Raport Płatności Cyfrowe 2020, https://eizba.pl/wp-content/uploads/2020/12/Raport-Platnosci-cyfrowe-2020-10.12.2020.pdf, s. 11.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nologicznych. Finanse cyfrowe pomagają obywatelom i przedsiębiorstwom radzić sobie z bezprecedensową sytuacją spowodowaną pandemią COVID-19. Na przykład dzięki weryfikacji tożsamości online konsumenci mogą otwierać rachunki i uzyskiwać zdalny dostęp do wielu usług finansowych.

Ponieważ coraz więcej osób korzysta z usług finansowych online, a pracownicy sektora finansowego pracują również zdalnie, o wiele ważniejsze stało się zapewnienie bezpiecznego i niezawodnego działania infrastruktury cyfrowej.

Jak podkreśliła na początku 2020 r. Komisja Parlamentu Europejskiego[5], potwierdzając swoje słowa w styczniu 2021 r.[6], kiedy odniosła się do Planu Odbudowy – promowanie cyfrowej transformacji UE jest jej głównym priorytetem.

Europejski sektor finansowy może rozbudowywać wiele innowacyjnych projektów we wszystkich państwach członkowskich, m.in. wspierać rozwój w takich obszarach, jak technologia płatności cyfrowych. Upowszechnienie finansów cyfrowych przyczyni się do transformacji cyfrowej gospodarek i społeczeństwa Europy. Przyniesie to duże korzyści konsumentom i przedsiębiorstwom.

Usługi płatnicze odgrywają kluczową rolę w usługach finansowych, gdyż stanowią przełomowe innowacje i wspierają gospodarkę cyfrową. Rozwiązania płatności cyfrowych umożliwiają osobom fizycznym i firmom bezpieczne i wydajne przeprowadzanie transakcji. Są niezbędne do dokonywania płatności, rozliczania rachunków, spłacania pożyczek lub kredytów hipotecznych, przesyłania pieniędzy, wypłaty wynagrodzeń lub emerytur, a także do dokonywania płatności w sklepach i e-commerce.

Powinniśmy przyjąć, że technologiczna transformacja to preludium do zmian w wielu sektorach, a co za tym idzie do koniecznych wdrożeń rozwiązań, mających chronić tak dane, którymi technologia cyfrowa się posługuje, jak i wspierających działania procesów chroniący sektor finansowy przed przestępczością zorganizowaną.

7.2. ZMIANY PRAWNE NA POZIOMIE EUROPEJSKIM I KRAJOWYM

Nie ma wątpliwości, że zmiany prawne w zakresie AML i CFT stały się niemal codziennością wielu segmentów rynku i instytucji obowiązanych. Rok 2021 przyniósł nowe rozwiązania, regulacje i systemy związane z przeciwdziałaniem praniu

[5] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Kształtowanie cyfrowej przyszłości Europy", COM(2020) 67 final, 19 lutego 2020.

[6] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Decydujący moment dla Europy: naprawa i przygotowanie na następną generację", COM(2020) 456 final.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

pieniędzy. Od 15 maja 2021 r. obowiązuje część przepisów wprowadzonych ustawą zmieniającą ustawę o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu z 1 marca 2018 r.[7]. Nowelizacja dostosowuje polskie przepisy AML do tzw. 5 Dyrektywy Anti-Money Laundering[8].

Przypomnijmy, że zmiany te mają na celu przede wszystkim zwiększenie przejrzystości informacji o beneficjentach rzeczywistych podmiotów korporacyjnych oraz poprawę dostępu do informacji będących w posiadaniu instytucji obowiązanych przez instytucje powołane do zwalczania prania pieniędzy. Oznacza to, że instytucje obowiązane mają dodatkowe obowiązki w zakresie stosowania zabezpieczeń i ustalania beneficjentów rzeczywistych.

Ponadto wdrożone w 2021 r. zmiany prawne dotyczą również innych zagadnień, spośród których warto wymienić trzy:

- kontynuowana jest nowelizacja polskiej ustawy o przeciwdziałaniu praniu pieniędzy, która implementuje piątą dyrektywę i m.in. poszerza listę instytucji obowiązkowych.,
- uchwalony został projekt ustawy o systemie informacji finansowej – w I kwartale 2021 r.,
- Polska musi wdrożyć kompleksowe regulacje, aby lepiej i wszechstronniej chronić sygnalistów (do 17 grudnia 2021 r.).

W kontekście zmian, jakie planowane są przez Unię Europejską, wyraźne trendy regulacyjne w zakresie przeciwdziałania praniu pieniędzy są obecnie reprezentowane przez Komisję Europejską, która w swym komunikacie z 7 maja 2020 r. wypowiedziała się na temat kompleksowego planu działania UE w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu[9]. Zgodnie z komunikatem UE powinna wprowadzić zasadę zerowej tolerancji dla środków pochodzących z nielegalnych źródeł. Według komisji wzrost aktywności przestępczej w kontekście pandemii COVID-19 przypomina, że przestępcy będą wykorzystywać wszelkie możliwe środki do prowadzenia nielegalnych działań szkodzących społeczeństwu, a UE musi być równie zdeterminowana, aby uniemożliwić im czerpanie korzyści z tych występków.

[7] Zmiana przepisów o przeciwdziałaniu praniu pieniędzy. Nowe instytucje obowiązane i surowsze wymogi weryfikacji beneficjenta rzeczywistego, https://www.parp.gov.pl/component/content/article/73691:zmiana-przepisow-o-przeciwdzialaniu-praniu-pieniedzy-nowe-instytucje-obowiazane-i-surowsze-wymogi-weryfikacji-beneficjenta-rzeczywistego (data dostępu: 25 sierpnia 2021).

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.

[9] Projekt rezolucji w sprawie kompleksowej unijnej polityki zapobiegania praniu pieniędzy i finansowaniu terroryzmu – plan działania komisji i dalszy rozwój sytuacji, https://www.europarl.europa.eu/doceo/document/B-9-2020-0207_PL.html (data dostępu: 25 sierpnia 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Patrząc na czekające nas zmiany regulacyjne można wysunąć wnioski, że celem unijnych i krajowych inicjatyw jest zwiększenie transparentności i jednolitości danych oraz działań związanych z AML i CFT. Oto kilka przykładów:

- organy krajowe będą miały dostęp do większej ilości informacji, na przykład do Systemów Informacji Finansowej,
- Unia Europejska planuje stworzenie mechanizmu koordynującego i wspierającego współpracę między agencjami wywiadu finansowego państw członkowskich (FIU-Financial Intelligence Unit),
- nowelizacja ustawy o przeciwdziałaniu praniu pieniędzy przewiduje m.in. objęcie innych organizacji instytucjami obowiązanymi i nałożenie na nie nowych obowiązków,
- na poziomie UE zostanie utworzony system monitoringu, który usprawni przepływ informacji i zapewni wdrożenie wymagań UE w zakresie AML i CFT na jednolitym poziomie w państwach członkowskich[10].

7.3. GŁÓWNE TRENDY W INNOWACJACH CYFROWYCH

Proces transformacji cyfrowej przyspiesza i wiele branż staje się bardziej otwartych na współpracę w tej dziedzinie. Aplikacje technologiczne i cyfrowe są coraz częściej tworzone w sposób modułowy, dzięki czemu mogą komunikować się ze sobą za pomocą interfejsów programowania aplikacji. Mogą lepiej dostosować usługi do potrzeb klientów. Stwarzają również więcej możliwości eksperymentowania i współpracy między różnymi użytkownikami. Może to mieć wieloraki wpływ na sposób świadczenia usług finansowych. Wraz z infrastrukturą IT dane stają się kluczowym zasobem innowacyjnym. Obecnie dane, jakimi posługuje się rynek finansowy, są ważniejsze niż kiedykolwiek do tej pory. Dostępność danych cyfrowych pozwala na dokładniejsze przewidywanie przyszłych wydarzeń, umożliwiając świadczenie usług „szytych na miarę".

Analiza połączonych zestawów danych dostarcza więcej informacji niż analizowanie każdego zestawu danych osobno. Gdy wiele stron uzyskuje dostęp do określonego zestawu danych w tym samym czasie, korzyści ekonomiczne są większe. Ponadto, aby zmaksymalizować wartość danych, należy wykorzystać powiązane technologie. Obecnie infrastruktura IT coraz częściej znajduje się w chmurze, co zapewnia dużą elastyczność operacyjną i ułatwia dostęp do zaawansowanych technologii przetwarzania danych. Zmiany te rodzą również ważne nowe kwestie zwią-

[10] KNF, *Nowa ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – praktyczne ujęcie*, https://www.knf.gov.pl/knf/pl/komponenty/img/Prezentacja%20CEDUR%2016-05-2018_61908.pdf (data dostępu: 25 sierpnia 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

zane z ochroną konsumentów i odpowiedzialnym wykorzystywaniem ich danych osobowych.

Jednocześnie innowacyjność powoduje zmiany w strukturze rynku. W Europie powstało wiele udanych start-upów z branży FinTech. Istniejące firmy dokonały głębokich zmian w swoich modelach biznesowych, zwykle we współpracy z firmami z sektora technologii finansowych. Firmy technologiczne – zarówno duże (tzw. BigTech), jak i małe – są coraz bardziej aktywne w sektorze usług finansowych. Dynamiczny rozwój zmienia charakter zagrożeń, przed którymi stoją konsumenci, użytkownicy, i stabilność finansową, i może mieć przy tym znaczący wpływ na konkurencję w usługach finansowych.

Stosowanie nowych technologii ma duży wpływ na ryzyka, jakie generowane są przez nie same. Obecnie można wykorzystać zasoby komputerowe (serwery, bazy danych, oprogramowanie, pliki), które nie muszą być dostępne na komputerze lokalnym. Stosowanie rozwiązań chmurowych ma wpływ na poprawę mocy obliczeniowej systemów informatycznych i stanowi przełom w upowszechnieniu nowych zastosowań technologii cyfrowej. Rozwój samej chmury jako usługi jest kluczowym czynnikiem przyspieszającym cyfrową transformację firmy. Pozwala wykorzystać potencjał nowych technologii bez inwestowania w sprzęt i infrastrukturę.

Kluczowym czynnikiem w rozwoju chmury jest szybszy Internet. W 2019 r., w decydującą fazę weszło wdrożenie nowego standardu połączeń mobilnych 5G. Ta swego rodzaju rewolucja technologiczna zapewniła prędkość transferu danych do 100 GB/s, co zminimalizowało opóźnienia wynikające z przesyłu danych i, co ważniejsze, pozwoliło na łączenie w sieci znacznie większej ilości urządzeń. Tym samym rozwój technologii 5G przyczynił się do dynamicznego rozwoju Internetu Rzeczy – (IoT – *Internet of Things* lub *Intelligence of Things*) – w uproszczeniu system urządzeń elektronicznych, które mogą automatycznie komunikować się i wymieniać dane za pomocą sieci bez ingerencji człowieka[11].

Technologia ta pozwala dzięki zastosowaniu wielu czujników na budowanie inteligentnych pojazdów, budynków a nawet miast. Jednak urządzenia rejestrujące wszelkie przejawy osobistej aktywności nasycają środowisko, powodując wiele problemów związanych z bezpieczeństwem danych i ochroną prywatności użytkowników. Wyzwaniem staje się takie budowanie systemów nadzorujących, które w bezpieczny sposób przechowują i przetwarzają dane, jakimi się posługują.

Uzupełnieniem najnowszych trendów w technologii rozwijanej dla Internetu Rzeczy i Sztucznej Inteligencji jest technologia blockchain. Jak opisuje ją P. Adamczyk, są to transakcje przeprowadzane za pośrednictwem łańcucha bloków, które najpierw przesyłają żądania wykonania do innych uczestników za pośrednictwem sieci P2P (ang. *person-to-person*), a następnie algorytm używany w łańcuchu

[11] M. Jaskulski, *Co to jest Internet Rzeczy (IoT)?*, https://www.benchmark.pl/aktualnosci/co-to-jest-internet-rzeczy-iot.html (data dostępu: 26 sierpnia 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

blokowym automatycznie potwierdza transakcję. Transakcja jest łączona z innymi w celu utworzenia nowego bloku danych do rejestru. Blok danych zostaje automatycznie dodany do istniejącego bloku tworząc bezpieczny i niezmienny łańcuch. Cała transakcja na tym się kończy[12]. Początkowo blockchain był używany głównie do tworzenia kryptowalut (opierał się na kryptografii). Wkrótce jednak odkryto, że nowe technologie – charakteryzujące się bezpieczeństwem i szybkością transakcji oraz możliwością wyeliminowania pośredników – mogą zapewnić większe możliwości. Blockchain może być publiczny, otwarty dla każdego użytkownika (na przykład Bitcoin) lub prywatny i zamknięty, oraz dostępny tylko dla określonej grupy uczestników pracujących w określonej branży lub łańcuchu dostaw. Paradoksalnie głównym beneficjentem technologii blockchain może być system finansowy. Blockchain może uprościć i przyspieszać transgraniczny transfer wartości oraz wspierać przy wprowadzeniu bezpieczniejszych mechanizmów weryfikacji tożsamości[13].

Dzięki tej funkcji można zautomatyzować proces weryfikacji i autoryzacji odpowiednio ustrukturyzowanych dokumentów lub programów (takich jak weryfikacja tożsamości klienta czy weryfikacja klauzul umownych).

Podsumowując, technologia cyfrowa w znaczący sposób zmienia nasz świat, w tym również dynamicznie zmienia świat finansów, a właściwie można by użyć stwierdzenia, że go rewolucjonizuje.

7.4. STRATEGICZNE CELE FINANSÓW CYFROWYCH NA PODSTAWIE PROPOZYCJI KE

Sektor finansowy musi podążać za nowymi trendami i wykorzystać wszystkie możliwości, jakie daje rewolucja cyfrowa. Europa musi wspierać finanse cyfrowe, przy wiodącym udziale silnych europejskich uczestników rynku[14]. Celem tych działań jest umożliwienie konsumentom i przedsiębiorstwom czerpania korzyści z cyfrowego finansowania. Kraje członkowskie powinny promować finanse cyfrowe w oparciu o europejskie wartości i ścisły nadzór nad czynnikami ryzyka.

W strategii finansów cyfrowych sformułowanej przez Komisję Europejską[15] przygotowano ogólne wytyczne dotyczące tego, w jaki sposób Europa będzie

[12] P. Adamczyk; *Możliwości zastosowania technologii blockchain w sektorze finansowym*, http://www.kwartalnikrsk.pl/assets/rsk1-2018-adamczyk-mozliwosci-zastosowania-twchnologii-blockchain.pdfv (data dostępu: 27 sierpnia 2021).

[13] A.K. Piech, Ministerstwo Cyfryzacji, Warszawa 2016, kryptochemik.pl.

[14] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „W sprawie strategii dla UE w zakresie finansów cyfrowych", COM(2020) 591 final (data dostępu: 24 września 2020).

[15] Komisja Europejska, Digital finance package, https://ec.europa.eu/info/publications/200924-digital-finance-proposals_pl.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wspierać cyfrową transformację finansów, jednocześnie dostosowując ryzyko, jakie wiązało się będzie z transformacją w nadchodzących latach. W strategii określono cztery główne priorytety:

- wyeliminowanie rozdrobnienia jednolitego rynku cyfrowego,
- dostosowanie ram regulacyjnych UE w celu promowania innowacji cyfrowych,
- promowanie finansowania opartego na danych,
- stawienie czoła wyzwaniom i zagrożeniom transformacji cyfrowej, w tym poprawa odporności operacji cyfrowych realizowanych przez instytucje finansowe.

Zdaniem komisji, przyjęcie rozwiązań pozwalających na rozwój finansów cyfrowych, uwolni innowacje w Europie i stworzy możliwości rozwoju lepszych produktów finansowych dla konsumentów (w tym dla tych, którzy obecnie nie mają dostępu do usług finansowych). Otworzy nowe możliwości dostarczania funduszy unijnym firmom, zwłaszcza małym i średnim przedsiębiorstwom. Ponieważ czynności oparte na finansach cyfrowych przyspieszają operacje transgraniczne, mogą również wzmocnić integrację rynków finansowych bankowości i unii rynków kapitałowych, wzmacniając tym samym Europejską Unię Gospodarczą i Walutową

Silny i dynamiczny (europejski i polski) cyfrowy sektor finansowy, umocni dzięki transformacji cyfrowej, swój potencjał do nasilenia otwartej autonomii strategicznej, wzmacniając tym samym swoją zdolność do monitorowania i nadzorowania systemu finansowego w celu ochrony stabilności finansowej.

Firmy technologiczne odgrywają coraz większą rolę w sektorze finansowym, zarówno jako dostawcy IT dla firm finansowych, jak i niezależni dostawcy usług finansowych. Regulacje dotyczące Digital Operational Resilience Act (DORA)[16], są zatem wprowadzane w celu zapewnienia wszystkim uczestnikom systemu finansowego niezbędnych zabezpieczeń, pozwalających na zminimalizowanie cyberataków i innych zagrożeń, jakie dotykają sektor IT. Przepisy te wymagają, aby wszystkie firmy były w stanie wytrzymać wszelkiego rodzaju przerwy i zagrożenia związane z technologiami informacyjno-komunikacyjnymi (ICT). Wprowadzają one również ramy regulujące dostawców usług ICT, takich jak dostawcy usług przetwarzania w chmurze.

Działania związane z szyfrowaniem (łańcuchem bloków) i powiązana z nimi technologia blockchain mogą stworzyć duże możliwości w sektorze finansowym, w tym: potencjalne tanie i szybkie płatności, transakcje transgraniczne i międzynarodowe, a także tworzyć nowe możliwości finansowania dla MŚP oraz dostarczać bardziej efektywny kapitał rynkowy. Tokeny użytkowe mogą umożliwić zdecentralizowanym sieciom działanie w technologii blockchain, a stabilne kryp-

[16] Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, https://ec.europa.eu/info/sites/info/files/180308-action-plan-FinTech_en.pdf.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

towaluty mogą stanowić podstawową formę płatności w branży mobilnej, energetycznej i produkcyjnej. Jednak wiążą się one również z ryzykiem i dlatego powinny podlegać odpowiedniemu nadzorowi. W ramach strategii odnoszącej się do kryptoaktywów, rynek powinien oczekiwać wsparcia KE, która wprowadziła już system pilotażowy dotyczący zaszyfrowanych zasobów, obejmując go nowymi przepisami, których ramy prawne ustanowiono na podstawie taksonomii dotyczącej różnych rodzajów zaszyfrowanych zasobów[17].

7.5. PRIORYTETY I POWIĄZANE DZIAŁANIA, ABY UMOŻLIWIĆ KONSUMENTOM I PRZEDSIĘBIORSTWOM CZERPANIE KORZYŚCI Z TECHNOLOGII CYFROWYCH FINANSÓW

Komisja Europejska wielokrotnie zajmowała się tematyką z zakresu finansów cyfrowych, nakreślając strategię dla Unii Europejskiej i wskazując priorytety, jakie państwa członkowskie powinny przyjąć w tej dziedzinie.

Spośród priorytetów zarysowanych przez KE możemy wyróżnić cztery:

- pierwszym zadaniem jest wyeliminowanie fragmentacji jednolitego rynku cyfrowego usług finansowych, co umożliwi konsumentom korzystanie z usług transgranicznych i pomoże nowoczesnym firmom finansowym rozszerzyć skalę działalności w środowisku cyfrowym. Firmy, które osiągają ekonomię skali, mogą również świadczyć takie usługi po niższych kosztach, zapewniając jednocześnie ich wyższą jakość,
- drugim priorytetem jest zapewnienie, aby ramy regulacyjne UE promowały innowacje cyfrowe, które leżą w interesie konsumentów i promują wydajność rynku. Innowacje oparte na technologii rozproszonego rejestru lub sztucznej inteligencji oraz wykorzystujące je mogą potencjalnie poprawić usługi finansowe dla konsumentów i przedsiębiorstw. Ramy regulacyjne dotyczące usług finansowych powinny zapewniać odpowiedzialne korzystanie z nich, zgodnie z wartościami UE. Szerszy, szybszy, bardziej otwarty i oparty na współpracy cykl innowacji wymaga regularnego przeglądu i analizy przepisów i praktyk UE dotyczących usług finansowych, aby zapewnić, że wspierają one innowacje cyfrowe oraz pozostaną odpowiednie i odpowiednie w ciągle zmieniającym się otoczeniu rynkowym,

[17] Sprawozdanie zawierające zalecenia dla komisji w sprawie finansów cyfrowych: pojawiające się ryzyko związane z kryptoaktywami – wyzwania w zakresie regulacji i nadzoru w obszarze usług, instytucji i rynków finansowych (2020/2034(INL).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- trzeci priorytet polega na stworzeniu europejskiej przestrzeni danych finansowych, której celem jest promowanie innowacji opartych na danych w oparciu o europejską strategię dotyczącą danych, w tym zwiększenie dostępu do danych i wymiany danych w sektorze finansowym. Przedstawiciele UE są zdania, że firmy, w tym firmy finansowe, powinny udostępniać kompleksowe informacje finansowe i niefinansowe dotyczące ich działalności i produktów. Poczynając od udostępniania danych dotyczących rachunków płatniczych w ramach zmienionej dyrektywy o usługach płatniczych, dalsze wysiłki kieruje na rzecz zwiększenia udostępniania danych i otwartości w innych sektorach gospodarki – przy jednoczesnym przestrzeganiu zasad ochrony danych i konkurencji – umożliwiając tym samym sektorowi finansowemu pełne wdrożenie innowacji opartych na danych. Takie działanie powinno zachęcić firmy do opracowywania innowacyjnych produktów dla konsumentów i przedsiębiorstw. KE proponuje przy tym pomoc we wspieraniu bardziej ogólnych celów polityki, takich jak ustanowienie jednolitego rynku danych,
- czwartym i zapewne najważniejszym zadaniem, jakiemu system finansowy powinien sprostać w najbliższym czasie, jest radzenie sobie z wyzwaniami i zagrożeniami transformacji cyfrowej.

Usługi finansowe migrują do środowiska cyfrowego o rozdrobnionym ekosystemie, w tym niektórych połączonych dostawców usług cyfrowych, którzy nie podlegają regulacjom finansowym i nadzorowi finansowemu. Dlatego mając na uwadze obecnie obowiązujące ramy prawne, finanse cyfrowe realizowane przez te podmioty mogą utrudnić utrzymanie stabilności finansowej, ochronę konsumentów, integralność rynku, a także utrzymanie uczciwej konkurencji i bezpieczeństwa. Aby zapewnić, że finanse cyfrowe będą pomagały tworzyć lepsze produkty finansowe dla konsumentów i przedsiębiorstw, należy wziąć pod uwagę te zagrożenia[18].

Odnosząc się do wszystkich czterech priorytetów, KE zwraca szczególną uwagę na promowanie nowych możliwości, jakie finanse cyfrowe zapewniają konsumentom oraz w stosownych przypadkach, szczególnie promuje działania dotyczące ochrony konsumentów. Odbywa się to z zachowaniem odpowiedniej zgodności z przepisami o ochronie danych, w szczególności z ogólnym rozporządzeniem o ochronie danych[19] (RODO).

[18] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „W sprawie strategii dla UE w zakresie finansów cyfrowych", COM(2020) 591 final (data dostępu: 24 września 2020).

[19] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

7.6. ROZWÓJ ZAUTOMATYZOWANYCH TECHNOLOGII WSPIERAJĄCYCH AML I CFT

Żyjemy w epoce szybkiego rozwoju technologii, innowacji, sztucznej inteligencji i uczenia maszynowego. Dotyczy to również zwalczania prania pieniędzy i finansowania terroryzmu. Systemy analizy przeciwdziałania praniu brudnych pieniędzy już istnieją i wciąż się rozwijają. Mają wbudowane wszystkie niezbędne elementy, aby zapewnić pełną zgodność z prawem i maksymalną automatyzację procesów.

Możemy wśród nich wymienić:

- ocena ryzyka prania pieniędzy,
- wewnętrzne procedury przeciwdziałania praniu pieniędzy,
- analiza i weryfikacja transakcji podmiotu,
- podejrzane transakcje i zgłoszenia transakcji powyżej progu.

Dzięki nowoczesnej technologii nawet najmniejsza instytucja obowiązana może skorzystać z profesjonalnych rozwiązań przeciwdziałających praniu pieniędzy. Dzięki temu mogą skuteczniej zwalczać przestępczość, zapewniając jednocześnie firmom i klientom większą dokładność, wydajność i bezpieczeństwo.

Przykłady możliwości, jakimi nowoczesna technologia wspiera instytucje, zestawiono w tabeli 1.

Analiza dostępnych systemów potwierdza, że są one w stanie skutecznie wspierać procesy AML i CFT, nie tylko pomagając przy wdrażaniu i integrowaniu nowoczesnych technologii, ale także znacząco wpływając na zasoby potrzebne do realizacji zadań, jakie wynikają z konieczności przeciwdziałania przestępczości zorganizowanej i praniu pieniędzy.

Tabela 1. Oprogramowanie wspierające procesy AML/CFT – 25 przykładów

Oprogramowanie	Opis
iComplyKYC	iComplyKYC to rozwiązanie zapobiegające praniu pieniędzy (AML) zaprojektowane, aby pomóc firmom zautomatyzować zgodność procesów związanych z finansowaniem cyfrowym. Umożliwia dostawcom usług finansowych zbieranie lub analizowanie danych KYC, wdrażanie klientów i zarządzanie ryzykiem w całym cyklu życia klienta.
Clear View KYC	Clear View KYC to oparte na chmurze oprogramowanie zapobiegające praniu pieniędzy (AML), zaprojektowane, aby pomóc bankom, instytucjom finansowym, dostawcom usług płatniczych (PSP) i kasynom w zapobieganiu przestępstwom finansowym i działaniom związanym z finansowaniem terroryzmu (CTF).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

GetID	GetID to rozwiązanie, które pomaga przyspieszyć proces onboardingu klienta, zapewnia pełną zgodność z przepisami i ogranicza oszustwa.
Token of Trust	Token of Trust to oparte na chmurze rozwiązanie zapobiegające praniu pieniędzy, które ma pomóc sprzedawcom internetowym w uwierzytelnianiu danych i weryfikowaniu tożsamości osób. Gromadzi informacje z wielu źródeł w ujednoliconej bazie danych, umożliwiając użytkownikom kojarzenie zachowań z prawdziwymi i możliwymi do zidentyfikowania osobami.
NameScan	NameScan to oprogramowanie zapobiegające praniu pieniędzy (AML) zaprojektowane, aby pomóc firmom z branży nieruchomości, prawa i innych w zapobieganiu przestępstwom finansowym i finansowaniu terroryzmu (CTF). Umożliwia organizacjom usprawnienie zgodności z AML za pomocą funkcji kontroli niepożądanych mediów.
DCS AML	DCS AML to oparte na chmurze oprogramowanie zapobiegające praniu brudnych pieniędzy, zaprojektowane, aby pomóc firmom usprawnić monitorowanie transakcji, zarządzanie ryzykiem i operacje onboardingu klientów. Umożliwia organizacjom zapewnienie zgodności z przepisami branżowymi i generowanie raportów o podejrzanej aktywności (SAR) przy użyciu modeli matematycznych i technologii sztucznej inteligencji (AI).
Ondato	Ondato to oparte na chmurze rozwiązanie do zarządzania zgodnością dla instytucji finansowych, które zapewnia narzędzia do weryfikacji tożsamości, wprowadzania klientów, walidacji danych, uwierzytelniania i nie tylko. Zestaw narzędzi obejmuje weryfikację tożsamości za pomocą zdjęć i filmów, uwierzytelnianie biometryczne twarzy i wiele innych.
Global-Gateway	GlobalGateway to platforma przeciwdziałająca praniu pieniędzy (AML) i weryfikacji tożsamości dla firm z różnych branż, w tym usług finansowych, handlu elektronicznego, handlu detalicznego, opieki zdrowotnej i administracji rządowej. Pomaga firmom zarządzać zgodnością, ograniczać oszustwa i budować zaufanie potencjalnych klientów.
SmartSearch	SmartSearch to oparte na chmurze rozwiązanie zapobiegające praniu pieniędzy (AML), zaprojektowane, aby pomóc firmom z branż, takich jak prawna, ubezpieczeniowa i księgowa, zachować zgodność i zapewnić ochronę finansową. Kluczowe funkcje obejmują monitorowanie klientów, alerty kredytowe, tworzenie przepływu pracy i raportowanie.
Socure	Wiodące rozwiązanie KYC/AML firmy Socure jest podstawową technologią dla firm poszukujących przewagi konkurencyjnej w pozyskiwaniu klientów, umożliwiając im natychmiastowe powiedzenie „tak" każdemu dobremu konsumentowi przy jednoczesnym zmniejszeniu ryzyka online.
TruNarrative	TruNarrative to oparte na chmurze rozwiązanie do wykrywania oszustw, zaprojektowane, aby pomóc firmom z branży bankowej, finansowej i handlu elektronicznego zachować zgodność podczas transakcji. Kluczowe funkcje obejmują weryfikację tożsamości, ocenę ryzyka, monitorowanie konta, eKYC, ścieżki audytu i zarządzanie sprawami.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Alessa	Jako rozwiązanie zapewniające zgodność z AML, Alessa oferuje analizę due diligence, sprawdzanie sankcji/list obserwacyjnych, monitorowanie/analizowanie/filtrowanie transakcji oraz automatyczne raportowanie regulacyjne dla różnych jurysdykcji. Zaawansowane analizy, przepływy pracy i zarządzanie sprawami wspierają kulturę zgodności.
Sanction Scanner	Sanction Scanner to oparte na sztucznej inteligencji oprogramowanie zgodne z AML. Zapewnia rozwiązania w zakresie kontroli AML i monitorowania transakcji, a także globalne usługi kontroli sankcji i PEP. Baza danych Sanction Scanner zawiera ponad 1500 sankcji. Obejmuje sankcje regulacyjne, egzekwowanie prawa i inne oficjalne globalne/lokalne sankcje. Sanction Scanner zawiera również listy motywacyjne i niepożądane dane medialne, w tym te wydawane przez USA, Wielką Brytanię, ONZ i inne globalne główne i mniejsze departamenty rządowe.
SAS Anti--Money Laundering	SAS zapewnia wysokowydajne analizy i wiele metod wykrywania, dzięki czemu można monitorować więcej zagrożeń i chronić reputację swojej instytucji. Przetwarza ponad 2 miliardy transakcji w ciągu jednej nocy. Testuje, dostosowuje i symuluje scenariusze w ciągu kilku sekund. Przetwarzanie tablicowe umożliwia monitorowanie wielu zagrożeń podczas jednego przebiegu danych, dzięki czemu można dodawać liczne scenariusze i czynniki ryzyka z niewielkim lub zerowym wpływem na czas przetwarzania.
Member-Check	MemberCheck to usługa zaprojektowana specjalnie dla pozabankowych branż finansowych, umożliwiająca podmiotom sprawozdawczym przestrzeganie przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w wydajny i opłacalny sposób. Wykorzystuje najbardziej szczegółową i dokładną obecnie dostępną globalną listę osób eksponowanych politycznie (PEP), oficjalnie sankcjonowanych osób i osób o szczególnym znaczeniu.
FAD	FAD to oprogramowanie w chmurze zaprojektowane, aby pomóc firmom zbierać, weryfikować i rejestrować podpisy elektroniczne zgodnie z przepisami branżowymi. Menedżerowie mogą przechwytywać wideo klientów zdalnych podczas procesów podpisywania umowy, umożliwiając im uwierzytelnianie i weryfikację tożsamości użytkowników końcowych.
Oracle AML and Financial Crime Compliance Management	Udostępnia platformę korporacyjną umożliwiającą skuteczne wykrywanie, prowadzenie dochodzeń i zgłaszanie podejrzeń o pranie pieniędzy i finansowanie terroryzmu. Rozwiązanie umożliwia organizacjom takim jak banki, firmy maklerskie i firmy ubezpieczeniowe codzienne monitorowanie transakcji klientów.
TaxCalc	TaxCalc to rozwiązanie do zarządzania praktykami podatkowymi, które ma pomóc księgowym, doradcom podatkowym i specjalistom ds. finansów w zarządzaniu klientami, obliczaniu zeznań podatkowych, przygotowywaniu sprawozdań finansowych i nie tylko. Umożliwia zespołom finansowym składanie deklaracji podatkowych klientów, weryfikowanie wpisów i monitorowanie terminów płatności.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Face Match	FaceMatch to zestaw do tworzenia oprogramowania do aplikacji identyfikacji biometrycznej (twarzy). Wbudowany detektor na żywo wspiera zapobieganie podszywaniu się i oszustwom fotograficznym. Twarze można porównywać, rozpoznawać i weryfikować w czasie rzeczywistym. Nadaje się do przetwarzania w chmurze i brzegowych.
Forensic-Cloud	ForensicCloud to oparte na chmurze oprogramowanie do wykrywania oszustw finansowych, które ma pomóc bankom i firmom z branży usług finansowych identyfikować, agregować i eliminować ryzyko przy użyciu zastrzeżonego modelu scoringowego. Organizacje mogą gromadzić, weryfikować i weryfikować dane klientów w celu prowadzenia dochodzeń w sprawie poznania klienta (KYC) oraz zapobiegania praniu pieniędzy, oszustwom i naruszeniom zgodności z poziomu ujednoliconej platformy.
Fraudio	Fraudio to pionierskie, oparte na chmurze rozwiązanie SaaS zaprojektowane do zwalczania złożonych oszustw płatniczych i przestępstw finansowych przy użyciu sztucznej inteligencji, uczenia maszynowego i efektów sieciowych obejmujących wiele zbiorów danych.
Merlon	Merlon to platforma badawcza przeciwdziałająca praniu pieniędzy (AML), która pomaga firmom wykorzystywać technologię sztucznej inteligencji (AI) do identyfikowania i oceny ryzyka finansowego lub ryzyka KYC (Know Your Customer). Analitycy mogą rejestrować swoje notatki, decyzje i inne działania w celu utrzymania ścieżek audytu.
Pirani AML Suite	Pirani AML Suite to pakiet AML zaprojektowany, aby pomóc firmom zarządzać i usprawniać zapobieganie praniu pieniędzy i finansowaniu terroryzmu w całej organizacji. Oferuje różne moduły, w tym Pirani Risk AML, Pirani Intelligence, Pirani Risk Profile, Pirani Monitor i Pirani Compliance.
Tonbeller	TONBELLER zapewnia bankom rozwiązanie przeciwdziałające ryzyku prania pieniędzy. Alerty generowane przez system oparte są na danych klienta i ustawieniach określonych przez użytkownika w zależności od ryzyka. Funkcjonalność zarządzania sprawami wspiera procesy decyzyjne, takie jak unieważnienie podejrzenia, złożenie raportu.
Pascal	Pascal to oprogramowanie AML zaprojektowane, aby pomóc firmom z sektora finansowego korzystać z narzędzi obsługujących sztuczną inteligencję w celu zapobiegania oszustwom związanym z tożsamością. Rozwiązanie umożliwia administratorom identyfikację odpowiednich osób zwalczających pranie brudnych pieniędzy zgodnie ze standardami zgodności

Źródło: AML Software: https://www.getapp.com/finance-accounting-software/anti-money-laundering (data dostępu: 19 sierpnia 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

7.7. WYZWANIA ZWIĄZANE Z CYFRYZACJĄ I OCHRONĄ DANYCH OSOBOWYCH

W 2021 r. cyfryzacja po raz kolejny znacząco zmienia nasze życie zawodowe i osobiste, dlatego metody, procedury, rozwiązania i systemy przeciwdziałające praniu brudnych pieniędzy stosowane w instytucjach powiązanych, muszą być stale dostosowywane do nowych regulacji. Przykładowo w 2021 r. kluczowa jest lepsza ochrona nowych innowacyjnych produktów i usług cyfrowych przed ryzykiem włączenia ich w nielegalną działalność. Ważnym tematem jest również weryfikacja tożsamości cyfrowej, która jest przeprowadzana starannie w celu ochrony danych osobowych. Art. 52 projektu ustawy o przeciwdziałaniu praniu pieniędzy[20] wskazuje na zmianę polegającą na zastrzeżeniu, że osoby wykonujące obowiązki związane z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu powinny uczestniczyć w programach szkoleniowych w zakresie wypełniania tych obowiązków, z uwzględnieniem zagadnień związanych z ochroną danych osobowych. „Sztuczna inteligencja nie istnieje bez danych"[21], zatem wyzwania, jakie stoją przed najnowszymi rozwiązaniami technologicznymi, są duże, a w szczególności powinny uwzględniać aspekt związany z danymi osobowymi i ich skuteczną ochroną.

„Do 2024 r. Komisja, we współpracy z Europejskimi Urzędami Nadzoru, zamierza zapewnić jasność w odniesieniu do oczekiwań nadzorczych co do sposobu, w jaki należy stosować ramy legislacyjne dotyczące usług finansowych do rozwiązań wykorzystujących sztuczną inteligencję (AI)"[22]. Komisja Europejska zwróciła się do europejskich organów nadzorczych i Europejskiego Banku Centralnego o zbadanie możliwości opracowania wytycznych nadzorczych i nadzorczych dotyczących wykorzystania rozwiązań sztucznej inteligencji w sektorze finansowym. Wytyczne te powinny być spójne z przyszłymi wnioskami dotyczącymi nowych ram regulacyjnych SI planowanych na 2021 r. Europejscy regulatorzy opierają się na trwających pracach w tym obszarze, w tym rekomendacjach europejskiej branży ubezpieczeniowej oraz grupy ekspertów ds. etyki cyfrowej powołanej przez Unię Europejską. Administracja pracowniczych programów emerytalnych. Europejskie organy regulacyjne pracują nad wyjaśnieniem środków ograniczania ryzyka w celu korzystania z rozwiązań opartych na sztucznej inteligencji w sektorze finansowym UE w sposób bezpieczny, niezawodny i etyczny. Ogólne wyzwania dotyczące korzystania z narzędzi AI zgodnych z RODO

[20] Internetowy System Aktów Prawnych (ISAP): https://isap.sejm.gov.pl/.

[21] UODO, *Sztuczna inteligencja nie funkcjonuje bez danych*, https://uodo.gov.pl/pl/138/2010.

[22] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „W sprawie strategii dla UE w zakresie finansów cyfrowych", COM(2020) 591 final (data dostępu: 24 września 2020).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

7.8. ZAUTOMATYZOWANE FUNKCJONALNOŚCI W ZAKRESIE AML

Zwalczanie prania pieniędzy i finansowania terroryzmu to szczególny obszar prawa. Dlatego tylko rozwiązanie specjalnie ukierunkowane na ten problem może rzeczywiście przyczynić się do realizacji obowiązków w zakresie przeciwdziałania praniu pieniędzy. I tylko najlepsze z nich – takie jak system i AML – zawierają wszystkie elementy potrzebne do zapewnienia zgodności z prawem i maksymalnej automatyzacji działań przeciwdziałających praniu pieniędzy:

- informacje prawne pozwalają być na bieżąco z najnowszymi przepisami bez tracenia czasu na regularne przeszukiwanie wielu prawniczych baz danych,
- najnowsze szkolenia online learning AML nie tylko gwarantują dostęp do najnowszej wiedzy, ale są zawsze dostępne w dogodnym miejscu i czasie,
- ocena ryzyka AML uwzględnia wiele czynników na poziomie makro i mikro, w tym indywidualne standardy poszczególnych zobowiązań,
- wewnętrzne procedury AML są odpowiednie dla rodzajów instytucji obligatoryjnych dostępnych dla Twojej firmy,
- rejestr transakcji dokonywanych przez instytucje obowiązane prowadzony jest automatycznie w postaci kompletnej bazy danych,
- automatyczne monitorowanie transakcji, w tym wykrywanie i analiza złożonych wzorców w czasie rzeczywistym,
- automatyczna weryfikacja podmiotów (takich jak klienci czy dostawcy), w szczególności list sankcyjnych, rejestrów beneficjentów rzeczywistych czy list ostrzegawczych KNF,
- automatycznie wprowadzają i zgłaszają podejrzane i ponadprogowe transakcje oraz automatycznie generują raporty, np. do GIIF.

Warto zauważyć, że iAML to kompleksowy system, który weryfikuje podmioty, analizuje transakcje, prowadzi rejestry AML oraz generuje raporty do GIIF. Rozwiązanie jest szybkie, skuteczne i niezawodne, a jednocześnie uwzględnia możliwości finansowe instytucji obowiązanych. Wykorzystanie zautomatyzowanych rozwiązań dostępnych w systemie iAML minimalizuje ryzyko błędu ludzkiego i obniża koszty przestrzegania ustawy. Dzięki modułowej budowie i możliwości ustawień konfiguracyjnych, system iAML udostępnia użytkownikom (nawet osobom bez wiedzy technicznej) wiele praktycznych funkcji przyspieszających i ułatwiających procesy związane z przeciwdziałaniem praniu brudnych pieniędzy. Aplikacja wykorzystuje strukturę plików JPK do importowania danych z programów zewnętrznych (w tym programów księgowych). Program można dalej rozbudowywać, personalizować i integrować z innymi systemami informatycznymi. Analiza jest wykonywana z szybkością do 1000 transakcji na sekundę.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Bezpieczeństwo systemu jest gwarantowane przez transmisję SSL i zgodność z przepisami dotyczącymi danych osobowych[23].

7.9. AI VIA AML

Instytucje finansowe mogą wykorzystywać technologię sztucznej inteligencji na wiele sposobów, a przeciwdziałanie praniu pieniędzy (AML) jest jednym z głównych obszarów zainteresowania. Instytucje finansowe mogą wykorzystywać sztuczną inteligencję do analizowania dużych ilości danych, filtrowania fałszywych alarmów i identyfikowania złożonych zachowań przestępczych. Może identyfikować połączenia i wzorce, które są zbyt złożone, aby można je było wykryć za pomocą prostego monitorowania opartego na regułach lub ludzkich oczu. FI zdała sobie sprawę z potencjału wewnętrznej i zewnętrznej sztucznej inteligencji i zaczęła ją wykorzystywać. Według raportu Digital Bank 35% organizacji finansowych wdrożyło co najmniej jedno rozwiązanie uczenia maszynowego[24]. Sztuczna inteligencja może usprawnić branżę usług finansowych, pomagając identyfikować oszustwa, monitorować transakcje AML, sprawdzać sankcje i rozumieć kontrolę klienta (KYC).

Accenture Research i Frontier Economics w swoim raporcie[25] ocenił, w jaki sposób sztuczna inteligencja może zwiększyć zyski i innowacje w branży. Badanie porównało tempo wzrostu gospodarczego 16 branż i przewidziało wpływ sztucznej inteligencji (AI) na globalny wzrost gospodarczy do 2035 r. Badanie pokazuje, że im bardziej sztuczna inteligencja jest zintegrowana z procesem gospodarczym, tym większy potencjał wzrostu gospodarczego. Wartym odnotowania wnioskiem z raportu jest to, że do 2035 r. sztuczna inteligencja może ważyć wzrost gospodarczy wszystkich branż średnio o 1,7%. Informacja i komunikacja (4,8%), produkcja (4,4%) i usługi finansowe (4,3%) to trzy branże o najwyższym rocznym tempie wzrostu całkowitej wartości dodanej napędzanej przez sztuczną inteligencję w 2035 r.

Największą korzyścią dla usług finansowych wykorzystujących sztuczną inteligencję będzie zautomatyzowanie i ograniczenie błędów w codziennych ręcznych zadaniach, w tym ocenie kredytowej i zapytaniach klientów pierwszego poziomu.

[23] System analityczny AM, https://www.iaml.com.pl/system-analityczny/.

[24] *Digital Banking Maturity 2020 Jaka jest reakcja banków na cyfrową rewolucję?,* https://www2.deloitte.com/pl/pl/pages/financial-services/articles/digital-banking-maturity-2020.html (data dostępu: 29 sierpnia 2021).

[25] *Artificial Intelligence Will Enable 38% Profit Gains By 2035*, https://www.forbes.com/sites/louiscolumbus/2017/06/22/artificial-intelligence-will-enable-38-profit-gains-by-2035/?sh=5665610e1969#:~:text=bran%C5%BCy%20.%20Raport%20mo%C5%BCna-,pobra-%C4%87%20tutaj,-(28%20s.%2C%20PDF (data dostępu: 19 sierpnia 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Accenture przewiduje, że do 2035 r. usługi finansowe osiągną 1,2 tys. USD dodatkowej wartości brutto ze sprzedaży sztucznej inteligencji. Inne obszary automatyzacji usług finansowych obejmują automatyzację zapytań badania rynku za pomocą inteligentnych robotów, a także scoring i przegląd kredytów hipotecznych.

7.10. PODSUMOWANIE

Skuteczna ochrona przed cyberzagrożeniami jakie pojawiają się przy szybko rozwijającej się technologii, wymagają kolejnych przełomów technologicznych w obszarze cyberbezpieczeństwa w zakresie Internetu Rzeczy (IoT). Dzięki skoordynowanym działaniom wielu instytucji możliwe stanie się trwałe i efektywne zarządzanie podatnościami i zagrożeniami jakie wynikają z obrotu pieniądzem. Postawiony na wstępie rozdziału cel zakładał analizę technologii wspierających AML i CFT, co zostało zrealizowane w sposób wyczerpujący. Pozwoliło to na ustalenie potrzeb i zakresu wsparcia, jakimi dostępne na rynku narzędzia powinny się charakteryzować, aby sprostać wyzwaniom, które nakłada na sektor finansowy dynamiczna zmiana wynikająca z jego cyfryzacji. Dynamiczny w ostatnim okresie rozwój nowych technologii przetwarzania danych i związanych z nimi zagrożeń wynikających z cybertechnologii spowodowało, że dotychczasowy model ochrony państw, podmiotów państwowych, podmiotów prywatnych i obywateli stał się niestabilny. Cyfryzacja wpływa na zmiany w relacjach społecznych i gospodarczych, co oznacza konieczność podjęcia działań zapewniających bezpieczeństwo sieci. Działania te w kontekście AML i CFT obejmują nie tylko konieczność dostosowania norm prawnych, ale i określenie funkcjonalności dla narzędzi wspierających procesy analityczne związane z zapewnieniem ładu cyberprzestrzeni. W związku z wdrożeniem technologii 5G, rozwojem sztucznej inteligencji oraz Internetu Rzeczy koniecznym staje się zadbanie również o prawidłowe działanie narzędzi wspierających procesy, pozwalające na równie dokładną i szybką analizę zagrożeń, takich jak dynamiczna cyfryzacja naszego otoczenia.

Jednocześnie należy postawić tezę, że przy tak dynamicznym rozwoju technologii cyfrowych bez równie dynamicznego wsparcia ze strony systemów i zautomatyzowanych technologii, skuteczne zabezpieczenie sektora finansowego i przeciwdziałanie praniu pieniędzy i przestępczości zorganizowanej nie będzie możliwe.

Celem badań niniejszego rozdziału było ustalenie wymagań dla zautomatyzowanych technologii w ujęciu wsparcia dla procesów związanych z AML i CFT. Zestawienie dostępnego na rynku oprogramowania dostarcza niezbędnego do analizy materiału, dzięki któremu możemy wysunąć wniosek, że istniejące na rynku oprogramowanie jest w stanie sprostać wyzwaniom, jakie niesie za sobą rozwój cybertechnologii.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Należy jednak mieć na uwadze, iż tempo rozwoju, jakim charakteryzuje się przedmiot badań, jest z natury rzeczy bardzo dynamiczny. Co za tym idzie, należy prowadzić badania w tym zakresie i dokonywać oceny przydatności dostępnych narzędzi, potwierdzając tym samym, iż są one w stanie (lub nie) wspierać skutecznie procesy związane z przeciwdziałaniem praniu pieniędzy i przestępczości zorganizowanej przy jednoczesnej dbałości o przetwarzane w tych procesach dane.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Tomasz Talar
Wyższa Szkoła Gospodarki Euroregionalnej
w Józefowie

ROZDZIAŁ 8.

PROCEDURA AML W BIURACH RACHUNKOWYCH – WYBRANE ASPEKTY

8.1. UWAGI WPROWADZAJĄCE

Biura rachunkowe z procederem prania pieniędzy, rzadziej finansowania terroryzmu[1], mogą spotykać się stosunkowo często. Jednak sama identyfikacja procesu prania pieniędzy, nie tylko ze względu na trudności w interpretacji definicji, może okazać się czynnością skomplikowaną i tym samym obarczoną wieloma błędami. Stąd też pojawia się potrzeba próby wskazania przepisów regulujących zagadnienia związane z praniem pieniędzy i finansowaniem terroryzmu w kontekście głównie biur rachunkowych o niewielkich rozmiarach, na które to przepisy podmioty te powinny zwrócić szczególną uwagę. W związku z powyższym nadrzędnym celem tego rozdziału jest kolejno wskazanie zasad i trybu przeciwdziałania praniu pieniędzy uregulowanych w ustawodawstwie krajowym[2]. Zasady, o których mowa, w myśl polskiego ustawodawcy mają zapobiegać zjawisku wykorzystywania systemu finansowego do prania pieniędzy i finansowania terroryzmu. Z kolei od 31 lipca 2021 r. przedsiębiorcy, których podstawową działalnością gospodarczą jest świadczenie usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg

[1] Szerzej na temat przeciwdziałania finansowaniu terroryzmu: M. El Ghamari, *Przeciwdziałanie finansowaniu terroryzmu międzynarodowego* (w:) *Pieniądz i jego oddziaływanie na otoczenie*, red. P. Sitek, WSFiZ w Warszawie, Warszawa 2016 oraz M. El Ghamari, *Finansowanie terroryzmu międzynarodowego* (w:) *Pieniądz i jego oddziaływanie na otoczenie,* red. P. Sitek, WSFiZ w Warszawie, Warszawa 2016.

[2] Zob. J. Duży, *Pranie pieniędzy* (w:) *Zorganizowana przestępczość podatkowa w Polsce. Zwalczanie przestępczego nadużycia mechanizmów podatków VAT i akcyzowego*, Wolters Kluwer, Warszawa 2013.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego stały się instytucjami obowiązanymi, bez względu na wielkość jednostki czy wysokość obrotów.

8.2. BIURA RACHUNKOWE JAKO INSTYTUCJA OBOWIĄZANA

Ustawodawca w art. 2 u.p.p.p. definiuje w ust. 1 pojęcie instytucji obowiązanej poprzez enumeratywne wyliczenie podmiotów zobowiązanych do wypełniania obowiązków przewidzianych ustawą, określając tym samym zakres podmiotowy ustawy[3]. Oczywiście, zakres ten jest szeroki i obejmuje swoim zasięgiem instytucje finansowe nadzorowane, instytucje pożyczkowe, giełdy, kantory, portfele kryptowalut, pośredników ubezpieczeniowych, pośredników nieruchomości, zawody prawnicze, wirtualne biura, biura pośredniczące w zakładaniu spółek, podmioty prowadzące działalność w zakresie usługowego prowadzenia ksiąg rachunkowych, biura rachunkowe[4], podmioty hazardowe, przedsiębiorców. W myśl przepisów art. 2 u.p.p.p., status instytucji obowiązanej został nadany między innymi podmiotom świadczącym usługi polegające na:

- tworzeniu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej,
- pełnieniu funkcji członka zarządu lub umożliwianiu innej osobie pełnienia takiej funkcji lub podobnej funkcji w osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej,
- zapewnianiu siedziby, adresu prowadzenia działalności lub adresu korespondencyjnego oraz innych pokrewnych usług osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej.

Status instytucji obowiązanej został także nadany podmiotom prowadzącym działalność gospodarczą polegającą na świadczeniu usług w zakresie:

- wymiany pomiędzy walutami wirtualnymi i środkami płatniczymi,
- wymiany pomiędzy walutami wirtualnymi,
- pośrednictwie w wymianie (tzw. giełdy kryptowalut)[5].

[3] Zob. J.W. Wójcik, *Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Wolters Kluwer, Warszawa 2002.

[4] A. Sroga, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Obowiązki biur rachunkowych*, Infor, 2021, s. 9.

[5] Dotyczy zarówno podmiotów, które prowadzą działalność kantorową, a także te podmioty, które świadczą usługi za pośrednictwem wyspecjalizowanych w tym zakresie platform internetowych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Warto w tym miejscu zwrócić szczególną uwagę na pewną grupę instytucji obowiązanych, a mianowicie wirtualne biura, biura pośredniczące w zakładaniu spółek, doradcy podatkowi, podmioty prowadzące działalność w zakresie usługowego prowadzenia ksiąg rachunkowych, biegli rewidenci i biura rachunkowe czyli przedsiębiorcy których podstawową działalnością gospodarczą jest świadczenie usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego, niebędący innymi instytucjami obowiązanymi[6].

W art. 2 ust 1 pkt 15 u.p.p.p. ustawodawca stanowi, iż instytucjami zobowiązanymi są: doradcy podatkowi w zakresie czynności doradztwa podatkowego innych niż wymienione w pkt 14 oraz biegli rewidenci. Zatem zarówno doradcy podatkowi, jak i biegli rewidenci są instytucjami obowiązanymi przede wszystkim z racji posiadania uprawnień doradcy podatkowego lub biegłego rewidenta, bez względu na fakt, czy są przedsiębiorcami i czy ich działalność oprócz doradztwa podatkowego, czy, w przypadku biegłych rewidentów, uprawnień audytorskich, dotyczy prowadzenia biura rachunkowego.

Doniosłe znaczenie, choćby z faktu, że to nowa regulacja, zajmuje w tym akcie prawnym wspomniany już art. 2 ust. 1 pkt 15a) u.p.p.p., który stanowi, iż instytucją obowiązaną są przedsiębiorcy w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz.U. z 2021 r. poz. 162), których podstawową działalnością gospodarczą jest świadczenie usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego, niebędący innymi instytucjami obowiązanymi. Mowa tu zatem w sposób jednoznaczny o przedsiębiorcach świadczących pewien szczególny rodzaj usług. Są to podmioty świadczące szeroko rozumiane usługi prawno-księgowe. Wobec tego od 31 lipca 2021 r. wszystkie biura rachunkowe (bez względu na formę organizacyjno-prawną czy też rozmiar prowadzonej działalności, a także bez względu na liczbę osób zatrudnionych w jednostce oraz rodzaj świadczonych usług[7] – są zobowiązane do przestrzegania norm służących przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Ponieważ doradcy podatkowi stanowią grupę instytucji obowiązanych z tytułu innego niż wspomniana jednostka redakcyjna, mowa tu (choć nie w sposób bezpośredni) o biurach rachunkowych[8]. zakres instytucji obowiązanych został rozszerzony między innymi o biura rachunkowe nie świadczące usług rachunkowych z zakresu pełnej rachunkowości, ale wykonujących inne czynności doradztwa podatkowego nie będące czynnościami zarezerwowanymi dla doradców podatko-

[6] Art. 2, ust. 1, pkt 15a ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2021 r., poz. 1132 z późn. zm.).

[7] Jeśli te wpisują się w dyspozycje art. 2, ust. 1, pkt 15a u.p.p.p.

[8] Artykuł ten został dodany przez ustawę z 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r., poz. 815 ze zm.), która w tym zakresie obowiązuje od 31 lipca 2021 r.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wych. Należy tu wskazać na czynności doradztwa podatkowego, co do których nie ma wątpliwości, że stanowią katalog czynności zastrzeżonych *stricte* dla doradców podatkowych i do tych czynności zgodnie z art. 2 ust. 2 ustawy z dnia 5 lipca 1996 r. o doradztwie podatkowym (t.j. Dz.U. z 2020 r. poz. 130 z późn. zm.) (dalej: u.d.p.) zawodowe wykonywanie czynności, o których mowa w ust. 1 pkt 1, 4 i 5 zastrzeżone jest wyłącznie dla podmiotów uprawnionych w rozumieniu ustawy. I tak przepisy u.d.p. zastrzegają możliwość zawodowego wykonywania czynności dla podmiotów uprawnionych względem:

- udzielania porad, opinii i wyjaśnień z zakresu prawa podatkowego, celnego i egzekucji administracyjnej;
- reprezentacji podatników (płatników, inkasentów) w postępowaniu przed organami administracyjnymi oraz sądami administracyjnymi,
- wykonywania niezależnego audytu funkcji podatkowej.

Z kolei czynności w zakresie:

- prowadzenia, w imieniu i na rzecz podatników, płatników i inkasentów, ksiąg rachunkowych, ksiąg podatkowych i innych ewidencji do celów podatkowych oraz udzielanie im pomocy w tym zakresie;
- sporządzania, w imieniu i na rzecz podatników, płatników i inkasentów, zeznań i deklaracji podatkowych oraz udzielania im pomocy w tym zakresie,

są czynnościami doradztwa podatkowego, ale ich wykonywanie nie jest zastrzeżone wyłącznie dla podmiotów uprawnionych[9].

Bez wątpienia należy zwrócić w tym miejscu uwagę na wydaną 9 kwietnia 2014 r. przez ministra finansów interpretację ogólną odnoszącą się między innymi do problematyki usług doradztwa podatkowego[10]. Wprawdzie interpretacja dotyczy stosowania zwolnienia podmiotowego z VAT oraz obowiązku prowadzenia ewidencji przy zastosowaniu kas rejestrujących, wobec podmiotów wykonujących m.in. usługi związane z obsługą rachunkowo-księgową, to zawarte w dokumencie stanowisko Ministerstwa Finansów dotyczące zagadnień świadczenia usług doradztwa podatkowego również nie jest jednoznaczne i może wywoływać wiele wątpliwości interpretacyjnych. Należy zatem odnieść się bezpośrednio do przepisów u.d.p. w tym zakresie jednocześnie postulując o doprecyzowanie zakresu

[9] A. Bartosiewicz, *Deklaracje i zeznania wypełniane przez podmioty nie będące doradcami podatkowymi – obowiązek ewidencjonowania sprzedaży w kasie rejestrującej*, ABC, https://sip.lex.pl/#/publication/470013091/bartosiewicz-adam-deklaracje-i-zeznania-wypelniane-przez-podmioty-nie-bedace-doradcami.?cm=URELATIONS (data dostępu: 11 września 2021).

[10] Pismo z dnia 9 kwietnia 2015 r., wydane przez: Ministerstwo Finansów, PT3.8101.2.2015.AEW.16, Stosowanie zwolnienia podmiotowego z VAT oraz obowiązku prowadzenia ewidencji przy zastosowaniu kas rejestrujących, wobec podmiotów wykonujących m.in. usługi związane z obsługą rachunkowo-księgową, http://sip.mf.gov.pl. https://sip.lex.pl/#/guideline/184808357?cm=DOCUMENT (data dostępu: 11 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

usług świadczonych przez podmioty nie świadczące usług doradztwa podatkowego zarezerwowanych jedynie dla doradców podatkowych.

Od 10 sierpnia 2014 r. weszły w życie przepisy dotyczące deregulacji zawodu księgowego zawarte w ustawie z 9.05.2014 r. o ułatwieniu dostępu do wykonywania niektórych zawodów regulowanych[11]. Dzięki tym przepisom czynności z zakresu usługowego prowadzenia ksiąg rachunkowych może świadczyć każdy, kto: posiada zdolność do czynności prawnych i legitymuje się niekaralnością za przestępstwo przeciwko wiarygodności dokumentów, mieniu, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, za przestępstwa skarbowe oraz za przestępstwa polegające na nierzetelnym prowadzeniu ksiąg rachunkowych oraz posiada ubezpieczenie od odpowiedzialności cywilnej. Warto zwrócić uwagę na brak jakiegokolwiek wymogu, uzależniającego prowadzenie działalności wymagającej posiadania specjalistycznej wiedzy, dla prowadzenia działalności w zakresie usług rachunkowo-księgowych. Stan taki może doprowadzić do dalekosiężnych, negatywnych skutków powierzenia prowadzenia ksiąg rachunkowych i podatkowych jednostkom nienależycie przygotowanym do wykonywania tak odpowiedzialnych czynności. Oczywiście stan taki ma swoje bezpośrednie odniesienie na jakość wypełniania obowiązków nałożonych na podmioty obowiązane (w tym biura rachunkowe) w przepisach u.p.p.p. Należy zatem w tym miejscu postulować zmianę prawa w tym zakresie. Ustawowe zdefiniowanie zawodu księgowego i określenie czynności księgowych nie stanowiących czynności doradztwa podatkowego zastrzeżonych doradcom podatkowym wyeliminowałoby zapewne spory interpretacyjne pomiędzy środowiskiem biur rachunkowych, a doradcami podatkowymi.

8.3. OGÓLNA OCENA RYZYKA W BIURZE RACHUNKOWYM

Każda instytucja obowiązana, w tym biura rachunkowe, ma obowiązek identyfikacji oraz oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu odnoszący się bezpośrednio do działalności tych instytucji[12]. Należy zwrócić uwagę, że jest to ocena stopnia, w jakim dana instytucja jest podatna na wykorzystanie w procederze prania bądź finansowania terroryzmu[13]. Jednocześnie

[11] Ustawa z dnia 9 maja 2014 r. o ułatwieniu dostępu do wykonywania niektórych zawodów regulowanych (Dz.U. poz. 768).

[12] Obowiązek ten wprost wynika z dyspozycji art. 27 ust. 1 u.p.p.p.

[13] Jak wskazuje preambuła dyrektywy AML „Ryzyko prania pieniędzy i finansowania terroryzmu nie jest takie samo w każdym przypadku. W związku z tym należy stosować całościowe podejście oparte na analizie ryzyka. Podejście oparte na analizie ryzyka nie jest wariantem nadmiernie liberalnym dla państw członkowskich i podmiotów zobowiązanych. Obejmuje ono podejmowanie

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

przy ocenie tej należy uwzględnić czynniki ryzyka dotyczące klientów, państw lub obszarów geograficznych, produktów, usług, transakcji lub kanałów ich dostaw[14]. Co ważne, jak stanowi norma art. 27 ust. 2 u.p.p.p., w trakcie dokonywania oceny ryzyka, instytucje obowiązane mogą uwzględniać obowiązującą krajową ocenę ryzyka[15], a także sprawozdanie Komisji Europejskiej, o którym mowa w art. 6 ust. 1–3 dyrektywy 2015/849[16]. Przy czym działania te mają być proporcjonalne do charakteru i wielkości instytucji obowiązanej. Jednak jeżeli podmiot posiada status instytucji obowiązanej, to powinien wypełniać obowiązki przewidziane w ustawie niezależnie od formy prowadzonej działalności, ilości posiadanych klientów, czy też ilości pracowników zatrudnionych w instytucji obowiązanej. Co za tym idzie, osoba fizyczna prowadząca samodzielnie jednoosobowe biuro rachunkowe, ma na gruncie ustawy takie same obowiązki jak duży bank. Również w zakresie sporządzenia właściwej oceny ryzyka.

Praktyczne wskazówki dotyczące sposobu przeprowadzenia oceny ryzyka każdej instytucji obowiązanej (w tym biur rachunkowych) określa także Urząd Komisji Nadzoru Finansowego (dalej: UKNF)[17]. Wskazuje na czynniki ryzyka podlegające ocenie[18], źródła informacji[19], a także metodykę i strukturę oceny

decyzji w oparciu o dowody w celu efektywniejszej identyfikacji ryzyka prania pieniędzy i finansowania terroryzmu zagrażających Unii oraz podmiotom prowadzącym działalność na jej terytorium".

[14] M. Karpiuk, *Pranie pieniędzy jako zjawisko zagrażające bezpieczeństwu i porządkowi publicznemu* (w:) *Problematyka polskiego pieniądza*, red. P. Sitek, WSFiZ w Warszawie, Warszawa 2015.

[15] Zgodnie z normą art. 25 u.p.p.p. obowiązek opracowania krajowej oceny ryzyka spoczywa na Generalnym Inspektorze Informacji Finansowej, we współpracy z Komitetem Bezpieczeństwa Finansowego. Jednocześnie Generalny Inspektor jest zobowiązany do weryfikacji aktualności i w razie potrzeby, jednak nie rzadziej niż co 2 lata, opracowania nowej, uwzględniającej aktualne zagadnienia, krajowej oceny ryzyka. Aktualna krajowa ocena ryzyka została opracowana w 2019 r. Należy zatem oczekiwać, że Główny Inspektor, zobowiązany na gruncie przepisów u.p.p.p., opracuje i opublikuje dokument, który powinien być datowany na 2021 r.

[16] Zob. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. UE. L. z 2015 r., nr 141, s. 73 z późn. zm.).

[17] Pismo z dnia 15 kwietnia 2020 r., wydane przez: Urząd Komisji Nadzoru Finansowego, Stanowisko dotyczące oceny ryzyka instytucji obowiązanej, www.knf.gov.pl. https://sip.lex.pl/#/guideline/185085662/stanowisko-dotyczace-oceny-ryzyka-instytucji-obowiazanej-pismo-wydane-przez-urzad-komisji-nadzoru.?cm=URELATIONS (data dostępu: 18 września 2021).

[18] Jako czynniki ryzyka podlegające ocenie UKNF wskazuje takie elementy, jak, np. narzędzia i systemy informatyczne wykorzystywane przez instytucję obowiązaną, stopień uzależnienia instytucji obowiązanej w obszarze związanym z AML/CFT od dostawców zewnętrznych, outsourcing procesów związanych z AML/CFT, skala rotacji pracowników oraz kierownictwa jednostek odpowiedzialnych za procesy AML/CFT, planowane przez instytucję obowiązaną zmiany w działalności biznesowej…

[19] Wśród źródeł informacji warto zwrócić uwagę choćby na: stanowiska lub komunikaty odpowiednich organów, takich jak: UKNF, Generalny Inspektor Informacji Finansowej (GIIF), Narodo-

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ryzyka[20]. W załączniku nr 1 do dokumentu UKNF prezentuje przykłady obszarów powiązanych z poszczególnymi czynnikami ryzyka wskazanymi w art. 27 ust. 1 ustawy, które powinny być uwzględnione w procesie oceny ryzyka.

Naturalnie zarówno czynniki ryzyka jak i obszary objęte analizą, wydaje się, powinny być przedmiotem analizy instytucji obowiązanej w kontekście jej wielkości i charakteru działalności. Nie każde bowiem biuro rachunkowe będzie świadczyło usługi na rzecz np. klientów emitujących akcje na okaziciela, czy też klientów, których prawa z akcji lub udziałów są wykonywane przez podmioty inne niż akcjonariusze lub udziałowcy. Warto jednak podkreślić, że w każdym przypadku stanowisko dotyczące oceny ryzyka instytucji obowiązanej UKNF stanowi doskonałe źródło wiedzy, w jaki sposób dokonać oceny ryzyka oraz jakie elementy przy jej tworzeniu, instytucja obowiązana powinna poddać szczegółowej analizie. Jak wskazuje sam ustawodawca w zdaniu drugim art. 27 ust. 1 u.p.p.p., „działania te są proporcjonalne do charakteru i wielkości instytucji obowiązanej". To istotna informacja. Przepis ten bowiem pozwala na pewnego rodzaju swobodę instytucji obowiązanej w kwestii tworzenia oceny ryzyka, uzależniając jej zakres do wielkości oraz charakteru samej instytucji.

Wskazany powyżej katalog czynników ryzyka stanowi, oczywiście, zbiór otwarty, a zakres i obszary objęte analizą mogą wzajemnie się przenikać i uzupełniać. Dla biur rachunkowych czynnikami ryzyka, które należy poddać szczególnej analizie, to np. unikanie płacenia przez klienta podatków lub innych danin publicznoprawnych, ukrywanie źródła pochodzenia środków pieniężnych lub innych aktywów. Należy też zwrócić szczególną uwagę na wszelkiego rodzaju naciski na natychmiastowe wykonanie operacji, a także dokonywanie darowizn lub innych przysporzeń majątkowych w sposób budzący wątpliwości co do celu, przeznaczenia środków.

Ważnym elementem oceny ryzyka każdego biura rachunkowego jest zatem określenie poziomu istotności ryzyka charakterystycznego dla danego przedsiębiorcy. Mówiąc inaczej, ocena ryzyka powinna pozwalać na określenie kontekstu działalności klienta, a także ryzyka, jakie może wynikać w związku z prowadzoną działalnością. Należy też wziąć pod uwagę zakres oferowanych usług biura rachunkowego czy też wskazanie scenariuszy ewentualnego wystąpienia danego ryzyka oraz ocenę prawdopodobieństwa ich wystąpienia, a także wywołanych skutków.

Ocena ryzyka to jedno z najważniejszych obowiązków nałożonych na instytucje obowiązane. To właśnie od rzetelności i rezultatu podjętych działań zależy

wy Bank Polski, opracowania Europejskich Urzędów Nadzoru, takich jak: Europejski Urząd Nadzoru Bankowego (EUNB), Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA), Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA).

[20] UKNF zwraca szczególną uwagę na ocenę ryzyka inherentnego, czyli ryzyka występującego w sytuacji braku działań podjętych w celu zmniejszenia prawdopodobieństwa wystąpienia ryzyka i/lub ograniczenia jego efektów, w odniesieniu do każdego czynnika ryzyka wymienionego w art. 27 ust. 1 u.p.p.p.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

poprawne określenie oraz zastosowanie środków bezpieczeństwa finansowego, które mają służyć wykorzystaniu instytucji obowiązanej w procederze prania pieniędzy czy też finansowania terroryzmu. Ocena ryzyka ma bezpośredni związek z kontrahentami instytucji obowiązanej, z którymi łączy ją na ogół stała współpraca. Dlatego też, nie wykluczając, oczywiście, transakcji okazjonalnych, instytucja obowiązana dokonuje oceny ryzyka praktycznie w sposób nieprzerwany. Trzeba jednak wskazać na normę art. 27 ust. 3 u.p.p.p., która bez względu na wielkość czy też charakter obliguje instytucję obowiązaną do aktualizacji oceny ryzyka nie rzadziej niż co dwa lata. Obowiązek weryfikacji i aktualizacji ma charakter bezwzględny. Instytucja obowiązana, która takiego obowiązku nie spełni, jednocześnie nie wypełnia dyspozycji zawartej w tej jednostce redakcyjnej.

Praktyka pokazuje, że określenie poziomu ryzyka powinno nastąpić przynajmniej w oparciu o skalę trójstopniową (ryzyko niskie, normalne, wysokie). W przypadku biur rachunkowych o bardziej skomplikowanym profilu działalności warto rozważyć stosowanie szerszej skali np. pięciostopniowej (ryzyko niskie, normalne, podwyższone, wysokie i nieakceptowalne).

Przepis art. 27 ust. 3 u.p.p.p. stanowi, aby instytucje obowiązane swoje oceny ryzyka sporządzały w formie papierowej lub elektronicznej. Wydaje się, że forma elektroniczna w tym względzie w znacznej mierze usprawni wypełnienie nałożonego na instytucję obowiązaną przez ustawodawcę obowiązku. Ten praktyczny aspekt pozwoli przede wszystkim niewielkim biurom rachunkowym na sprawne przeprowadzenie aktualizacji oceny ryzyka i bezpieczną jej archiwizację. Ocena ryzyka może zostać sporządzona w formie papierowej jako tzw. *check lista*, zawierająca odpowiednio katalog kryteriów wpisujących się w określony poziom ryzyka lub w postaci prostego formularza. Ocena ryzyka może zostać dokonana również w formie elektronicznej przy wykorzystaniu gotowych i kompletnych aplikacji lub programów analitycznych. Dostępność rozwiązań chmurowych, pozwalających na bezpieczne przechowywanie dokumentacji jest dziś stosunkowo duża. Trzeba jednak wskazać, że nie każde rozwiązanie zapewnia jednakowy poziom bezpieczeństwa danych. Stąd warto w tym zakresie podjąć działania zmierzające do wyboru raczej dedykowanych rozwiązań, przystosowanych dla odbiorców biznesowych.

Sporządzenie prawidłowej oceny ryzyka to bez wątpienia ogromne wyzwanie, przed którym stoją biura rachunkowe, szczególnie te biura, które od dnia 31 lipca 2021 r. dołączyły do podmiotów będących instytucjami obowiązanymi. Powinny one sporządzić ocenę ryzyka z uwzględnieniem wszystkich wymogów nakreślonych przez ustawodawcę. Ważnym dokumentem, pozwalającym na prawidłowe sporządzenie oceny ryzyka instytucji obowiązanej, jest „Stanowisko UKNF dotyczące oceny ryzyka instytucji obowiązanej" z 15 kwietnia 2020 r., w którym UKNF oprócz wskazania istoty oceny ryzyka, oraz sposobu jej przeprowadzenia,

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wskazuje także na najczęstsze błędy popełniane przez instytucje obowiązane podczas sporządzania oceny ryzyka[21].

8.4. ROZPOZNAWANIE RYZYKA PRANIA PIENIĘDZY ORAZ FINANSOWANIA TERRORYZMU W BIURACH RACHUNKOWYCH

Przepis art. 33 u.p.p.p. reguluje zasady rozpoznania przez instytucje obowiązane ryzyka prania pieniędzy oraz finansowania terroryzmu. W przepisie art. 33 ust. 1 ustawodawca w sposób ogólny określa obowiązek stosowania przez instytucje obowiązaną wobec swoich klientów środków bezpieczeństwa finansowego[22], jednocześnie nie definiuje w tej jednostce redakcyjnej samego pojęcia środków bezpieczeństwa finansowego. Biorąc jednak pod uwagę regulację zawartą w art. 33 ust. 2, instytucje obowiązane, w zakresie i z intensywnością uwzględniającymi rozpoznane ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz jego ocenę, rozpoznają ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz oceniają poziom rozpoznanego tego ryzyka[23]. Jednocześnie instytucje obowiązane dokumentują rozpoznane ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi[24] lub z transakcją okazjonalną[25] oraz jego ocenę, uwzględniając w szczególności czynniki dotyczące:

- rodzaju klienta,
- obszaru geograficznego,
- przeznaczenia rachunku,
- rodzaju produktów, usług i sposobów ich dystrybucji,

[21] Do najczęstszych błędów instytucji obowiązanej podczas sporządzania oceny ryzyka UKNF wskazuje: pominięcie niektórych czynników ryzyka wskazanych w art. 27 ust. 1 u.p.p.p., niewskazanie końcowych wniosków wynikających z oceny ryzyka, brak harmonogramu planowanych działań instytucji obowiązanej w celu ograniczenia ryzyka lub nieracjonalne terminy zawarte w harmonogramie działań oraz nieodpowiedni dobór metodyki, nie uwzględniający istotnych z punktu widzenia instytucji obowiązanej czynników ryzyka lub określający podatność na ryzyko w sposób nieadekwatny do skali i rodzaju działalności.

[22] Zob. art. 33, ust. 1 u.p.p.p.

[23] Art. 33, ust. 2 i 4 u.p.p.p.

[24] Poprzez stosunki gospodarcze należy rozumieć stosunki instytucji obowiązanej z klientem związane z jej działalnością zawodową i które w chwili ich nawiązywania wykazują cechę trwałości.

[25] Transakcją okazjonalną jest transakcja inna niż występująca w ramach stosunku gospodarczego, na ogół o charakterze krótkotrwałym lub jednorazowym.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- poziomu wartości majątkowych deponowanych przez klienta lub wartości przeprowadzonych transakcji,
- celu, regularności lub czasu trwania stosunków gospodarczych[26].

Samo sporządzenie oceny ryzyka nie musi być procesem skomplikowanym dla większości biur rachunkowych. Przeprowadzona przez instytucję obowiązaną analiza powinna uwzględniać co najmniej kilka czynników ryzyka dotyczących rodzaju obsługiwanych klientów, państw lub obszarów geograficznych, produktów, usług oraz kanałów dystrybucji. Wybrane czynniki ryzyka powinny zostać przeanalizowane i poddane ocenie, a następnie instytucja obowiązana powinna dokonać analizy prawdopodobieństwa wystąpienia zdarzeń objętych ryzykiem oraz ich skutków. Wśród czynników ryzyka dotyczących rodzaju klienta, a które najczęściej będą miały wpływ na indywidualną ocenę ryzyka, warto wskazać choćby na tak istotne elementy, jak:

- struktura własnościowa klienta (czy jest to osoba fizyczna, osoba prawna, jednostka organizacyjna nieposiadająca osobowości prawnej), ze szczególnym uwzględnieniem stopnia złożoności tej struktury,
- rodzaj prowadzonej działalności gospodarczej (w sposób szczególny należy tu uwzględnić działalność klientów działających w branżach, gdzie może nastąpić duże ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu np. obrót walutami wirtualnymi, działalność kantorowa,
- długość trwania relacji biznesowych,
- zapytania ze strony GIIF i/lub organów ścigania dotyczące klientów,
- brak możliwości identyfikacji klienta oraz weryfikacji jego tożsamości,
- brak możliwości ustalenia struktury własnościowej klienta.

Do czynników ryzyka dotyczących obszarów geograficznych zaliczyć można przede wszystkim:

- posiadanie przez klienta siedziby w państwie trzecim wysokiego ryzyka w rozumieniu art. 2 ust. 2 pkt 13 u.p.p.p.[27],
- dokonywanie przez klienta w sposób systematyczny transakcji z kontrahentami mającymi siedzibę w państwie wysokiego ryzyka,
- prowadzenie przez instytucję obowiązaną działalności w strefie przygranicznej lub w lokalizacjach, o których powszechnie wiadomo, że są wysoce narażone na ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu.

[26] Art. 33, ust 3 u.p.p.p.

[27] Będą to państwa o wysokim poziomie korupcji lub innego rodzaju działalności przestępczej czy też państwa, w stosunku do których Organizacja Narodów Zjednoczonych lub Unia Europejska podjęły decyzję o nałożeniu sankcji lub szczególnych środków ograniczających lub państwa stosujące szkodliwą konkurencję podatkową.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Jeśli chodzi z kolei o czynniki ryzyka dotyczące produktów i usług, warto zwrócić uwagę na:

- produkty umożliwiające wykonywanie transakcji gotówkowych, przede wszystkim transakcji opiewających na duże kwoty,
- produkty umożliwiające realizację transakcji transgranicznych,
- produkty o dużym stopniu złożoności,
- wykorzystanie produktów lub usług przez klienta w sposób nieadekwatny do istotnych zmian zachodzących w otoczeniu gospodarczym.

Czynniki ryzyka dotyczące przeprowadzanych transakcji to głównie:

- transakcje gotówkowe (np. kwota czy liczba transakcji gotówkowych),
- transakcje międzynarodowe, ze szczególnym uwzględnieniem transakcji powiązanych z krajami wysokiego ryzyka,
- transakcje przeprowadzane w ramach rachunków typu *nested*,
- tworzenie przez klientów kont rozliczeniowych o niewiadomym lub niejasnym przeznaczeniu.

Przepis ten koresponduje z kolejną jednostką redakcyjną u.p.p.p., która dookreśla zakres środków bezpieczeństwa finansowego, a więc z art. 34 u.p.p.p.

8.5. ŚRODKI BEZPIECZEŃSTWA FINANSOWEGO W BIURZE RACHUNKOWYM

Środki bezpieczeństwa finansowego powinny być podjęte przez instytucje obowiązane w sytuacjach określonych w art. 35 u.p.p.p. Dla instytucji obowiązanej (biura rachunkowego) jest to moment nawiązywania współpracy z nowym klientem bądź wystąpienia podejrzenia prania pieniędzy w związku z relacją lub transakcją z istniejącym klientem. Służą one przede wszystkim zapewnieniu instytucji obowiązanej bezpieczeństwa wewnętrznego. Obejmują swym zakresem identyfikację klienta oraz weryfikację jego tożsamości, identyfikację beneficjenta rzeczywistego, ocenę stosunków gospodarczych i, stosownie do sytuacji, uzyskanie informacji na temat ich celu i zamierzonego charakteru oraz bieżące monitorowanie stosunków gospodarczych klienta[28]. Identyfikacja klienta w przypadku osób fizycznych będzie polegała przede wszystkim na ustaleniu imienia i nazwiska, numeru PESEL, serii i numeru dokumentu tożsamości (dowodu osobistego lub paszportu), adresu zamieszkania, adresu prowadzenia działalności gospodarczej, a także numeru identyfikacji podatkowej (NIP). Z kolei w przypadku osoby prawnej oraz jednostki organizacyjnej nieposiadającej osobowości prawnej, dla identyfikacji

[28] Art. 34, ust. 1, pkt 1 u.p.p.p.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

klienta niezbędne wydaje się uzyskanie przez biuro takich danych jak firma osoby prawnej, informacja o siedzibie klienta oraz adresie prowadzenia działalności gospodarczej. Niezbędna też będzie wiedza na temat formy organizacyjnej klienta oraz uzyskanie wiedzy o danych zawartych w rejestrze handlowym takich jak: numer rejestru oraz data rejestracji, dane osobowe osób reprezentujących klienta.

Kolejnym elementem stanowiącym środek bezpieczeństwa finansowego jest identyfikacja beneficjenta rzeczywistego. Należy w tym miejscu dokonać próby zdefiniowania pojęcia beneficjenta rzeczywistego. Otóż ustawodawca w art. 2 ust. 2 pkt 1 definiuje beneficjenta rzeczywistego dla potrzeb u.p.p.p. jako każdą osobę fizyczną, która bezpośrednio lub pośrednio sprawuje kontrolę nad klientem poprzez posiadane uprawnienia umożliwiające tej osobie wywieranie decydującego wpływu na czynności lub działania podejmowane przez klienta, lub każdą osobę fizyczną, w imieniu której są nawiązywane stosunki gospodarcze lub jest przeprowadzana transakcja okazjonalna[29]. Zakres danych beneficjentów rzeczywistych gromadzonych obowiązkowo, został w obecnie obowiązującej u.p.p.p. ograniczony ze względu na fakt, że w większości przypadków instytucje obowiązane nie mają bezpośredniego kontaktu z beneficjentem rzeczywistym klienta. Jednocześnie nie są w stanie uzyskać danych związanych z tożsamością beneficjenta rzeczywistego, jakie mogą uzyskać w odniesieniu do danych osobowych swoich klientów. Ustawodawca jednak wskazuje na obowiązek podejmowania uzasadnionych czynności w celu weryfikacji tożsamości beneficjenta rzeczywistego, a także ustalenia struktury własności i kontroli – w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej. Identyfikacja beneficjenta rzeczywistego obejmuje zatem imię i nazwisko oraz obywatelstwo osoby fizycznej wpisującej się w definicję ustawową beneficjenta rzeczywistego. Naturalnie przypadku posiadania przez instytucję obowiązaną takich danych jak PESEL, data urodzenia, seria i numer dokumentu stwierdzającego tożsamość, adres zamieszkania, identyfikacja beneficjenta rzeczywistego obejmuje również te informacje.

Sama weryfikacja tożsamości klienta i beneficjenta rzeczywistego następuje przed nawiązaniem stosunków gospodarczych lub przeprowadzeniem transakcji okazjonalnej i może być zakończona podczas nawiązywania stosunków gospodarczych, jeżeli jest to konieczne dla zapewnienia ciągłości prowadzenia działalności gospodarczej i gdy występuje niskie ryzyko prania pieniędzy oraz finansowania terroryzmu[30].

W kontekście środków bezpieczeństwa finansowego należy wspomnieć o takich elementach jak: ocena stosunków gospodarczych i, stosownie do sytuacji, uzyskanie informacji na temat ich celu i zamierzonego charakteru, bieżącym moni-

[29] Art. 2, ust 2, pkt 1 u.p.p.p. wylicza w sposób enumeratywny podmioty będące beneficjentami rzeczywistymi.

[30] Możliwość taką daje zapis art. 39, ust 2 u.p.p.p.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

torowaniu stosunków gospodarczych klienta, a w tym: analizę transakcji przeprowadzanych w ramach stosunków gospodarczych w celu zapewnienia, że transakcje te są zgodne z wiedzą instytucji obowiązanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz zgodne z ryzykiem prania pieniędzy, a także finansowania terroryzmu związanym z tym klientem, badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta – w przypadkach uzasadnionych okolicznościami, a także zapewnienie, że posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych są na bieżąco aktualizowane.

Bezwzględnym obowiązkiem nakładanym przez ustawodawcę na instytucje obowiązane jest dokumentowanie stosowanych przez nią środków bezpieczeństwa. Obowiązek ten zawarty jest w art. 34 ust 3 u.p.p.p, który stanowi, że instytucje obowiązane dokumentują zastosowane środki bezpieczeństwa finansowego oraz wyniki bieżącej analizy przeprowadzanych transakcji. Jednocześnie w przypadku żądania organów, o których mowa w art. 130 ustawy instytucje obowiązane powinny wykazać, że przy uwzględnieniu poziomu rozpoznanego ryzyka związanego zastosowały odpowiednie środki bezpieczeństwa finansowego. Oczywiście, w trakcie dokonywania analizy czynników związanych z ryzykiem prania pieniędzy i finansowania terroryzmu instytucja obowiązana przetwarza dane osobowe klientów czy beneficjentów rzeczywistych. Dlatego też ustawodawca przewidując taką możliwość daje zgodę na przetwarzanie danych osobowych zawartych w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu. Instytucja obowiązana może sporządzać kopie tych danych[31]. Informację o przetwarzaniu danych osobowych instytucja obowiązana ma przekazać klientowi przed nawiązaniem stosunków gospodarczych lub przed przeprowadzeniem transakcji okazjonalnej[32].

Środki bezpieczeństwa finansowego są stosowane przez biura rachunkowe w szczególności w przypadku:

- nawiązywania stosunków gospodarczych,
- przeprowadzania transakcji okazjonalnej:
  - o równowartości 15 000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane, lub
  - która stanowi transfer środków pieniężnych na kwotę przekraczającą równowartość 1000 euro,

[31] Należy zaznaczyć, że art. 34, ust. 4 u.p.p.p. literalnie wskazuje na dane osobowe jedynie dwóch grup podmiotów, a mianowicie klientów oraz osób upoważnionych do działania w ich imieniu. W odniesieniu choćby do obowiązku identyfikacji beneficjenta rzeczywistego ustawodawca nie przekazuje instytucji obowiązanej takiego uprawnienia. Należy wobec tego zakładać, że skoro obowiązek identyfikacji klienta, podobnie jak obowiązek identyfikacji beneficjenta rzeczywistego mieści się w kategorii osób, które instytucja obowiązana ma obowiązek identyfikować, takie prawo przetwarzania danych osobowych obejmuje również dane beneficjenta rzeczywistego.

[32] Zob. art. 43, ust. 5 u.p.p.p.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- podejrzenia prania pieniędzy lub finansowania terroryzmu,
- wątpliwości co do prawdziwości lub kompletności dotychczas uzyskanych danych identyfikacyjnych klienta[33].

Dodatkowo ustawodawca wprowadza, oprócz wymienionych powyżej, dwie sytuacje, które nakładają obowiązek stosowania środków bezpieczeństwa finansowego dla określonej kategorii instytucji obowiązanych[34]. Są to:

- przeprowadzanie gotówkowej transakcji okazjonalnej o równowartości 10 000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane (jedynie w odniesieniu do przedsiębiorców przyjmujących wpłaty, o których mowa w art. 2 ust. 1 pkt 23 u.p.p.p.)[35],
- obstawianie stawek oraz odbioru wygranych o równowartości 2000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane (jedynie w przypadku instytucji obowiązanych, o których mowa w art. 2 ust. 1 pkt 20 u.p.p.p.)[36].

Przepisy u.p.p.p. dają możliwość, nienawiązywania relacji gospodarczych z klientami oraz nakazują wypowiadanie zawartych umów w przypadku niemożliwości wykonania któregokolwiek ze środków bezpieczeństwa finansowego, o których mowa w art. 34 ust. 1 u.p.p.p. Treść przepisu jednocześnie nakazuje, nawet jeśli wystąpi ryzyko braku możliwości zastosowania tylko jednego z wymienionych w ustawie środków bezpieczeństwa finansowego, nienawiązywanie stosunków gospodarczych oraz powstrzymanie się od przeprowadzenia jakiejkolwiek transakcji okazjonalnej, a także powstrzymania się od przeprowadzania transakcji za pośrednictwem rachunku bankowego i tym samym rozwiązanie stosunków gospodarczych z klientem[37]. Przy czym to do instytucji obowiązanej należy ocena, czy w takiej sytuacji zachodzi konieczność, a stan faktyczny to potwierdza, przekazania Generalnemu Inspektorowi zawiadomienia, o którym mowa w art. 74 u.p.p.p.p.[38] lub

[33] Art. 35, ust. 1 pkt 1 i 2 oraz 5 i 6.

[34] R. Obczyński (w:) *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Warszawa 2020, art. 35.

[35] Przepis art. 35 ust. 2 pkt 23 u.p.p.p. stanowi, że instytucjami obowiązanymi są przedsiębiorcy w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców w zakresie, w jakim przyjmują lub dokonują płatności za towary w gotówce o wartości równej lub przekraczającej równowartość 10 000 euro, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane.

[36] Art. 35, ust. 1, pkt 3 i 4.

[37] Zob. art. 41, ust. 1, pkt 1–4.

[38] Przepis art. 74, ust 1 lakonicznie stanowi, że „instytucja obowiązana zawiadamia Generalnego Inspektora o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu". Biorąc pod uwagę fakt, że przestępstwo prania pie-

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

art. 86 u.p.p.p.p.[39]. Niestety, wydaje się, że ustawodawca, szczególnie w odniesieniu do art. 86 u.p.p.p., nakłada na instytucję obowiązaną zadania, które co do zasady powinny wykonywać służby do tego typu zadań stworzone. Oczywiście, pracownicy biur rachunkowych mają możliwość wskazania wprost zdarzeń, które będą nosiły znamiona określonych w ustawie przypadków, które należy zgłosić Głównemu Inspektorowi. Nie należy jednak nakładać na instytucje obowiązane czynności zarezerwowanych dla służb skarbowych, celnych czy policji.

Biuro rachunkowe może zastosować pod pewnymi warunkami uproszczone środki bezpieczeństwa finansowego gdy ocena ryzyka potwierdza niższe ryzyko prania pieniędzy oraz finansowania terroryzmu, przy czym o niższym ryzyku świadczyć będzie w szczególności to, że klient jest:

- rezydentem państwa członkowskiego UE lub EFTA lub
- jednostką sektora finansów publicznych, o której mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2021 r. poz. 305)[40],
- przedsiębiorstwem państwowym albo spółką z większościowym udziałem Skarbu Państwa, jednostek samorządu terytorialnego lub ich związków,
- spółką, której papiery wartościowe są dopuszczone do obrotu na rynku regulowanym podlegającym wymogom ujawniania informacji o jej beneficjencie rzeczywistym, wynikającym z przepisów prawa Unii Europejskiej lub odpowiadającym im przepisom prawa państwa trzeciego, albo spółką z większościowym udziałem takiej spółki,
- rezydentem państwa trzeciego określanego przez wiarygodne źródła jako państwo o niskim poziomie korupcji lub innej działalności przestępczej, rezydentem państwa trzeciego, w którym według danych pochodzących z wiarygodnych źródeł obowiązują przepisy dotyczące przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu odpowiadające wymogom wynikającym z przepisów Unii Europejskiej z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

niędzy, że względu na trudności w jego typizacji jest trudne do bezspornego zdefiniowania, biura rachunkowe (szczególnie niewielkie podmioty) mogą mieć problem w kwestii konieczności wypełnienia tego obowiązku.

[39] Przepis art. 86, ust. 1 u.p.p.p. z kolei zawiera pojęcie nieostre „uzasadnionego podejrzenia".

[40] Są to organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały, jednostki samorządu terytorialnego oraz ich związki, związki metropolitalne, jednostki budżetowe, samorządowe zakłady budżetowe, agencje wykonawcze, instytucje gospodarki budżetowej, państwowe fundusze celowe, Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez prezesa Kasy Rolniczego Ubezpieczenia Społecznego, Narodowy Fundusz Zdrowia, samodzielne publiczne zakłady opieki zdrowotnej, uczelnie publiczne, Polską Akademię Nauk i tworzone przez nią jednostki organizacyjne, państwowe i samorządowe instytucje kultury, inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, instytutów działających w ramach Sieci Badawczej Łukasiewicz, banków oraz spółek prawa handlowego.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

O niższym ryzyku świadczyć będzie także:

- umowa ubezpieczenia na życie, w przypadku gdy składka roczna nie przekracza równowartości 1500 euro lub składka jednorazowa nie przekracza równowartości 3500 euro,
- przystąpienie i uczestnictwo w pracowniczym programie emerytalnym, zawarcie umowy i gromadzenie oszczędności na indywidualnym koncie emerytalnym lub indywidualnym koncie zabezpieczenia emerytalnego,
- oferowanie produktów lub usług w celu zapewnienia odpowiednio zdefiniowanego i ograniczonego dostępu do systemu finansowego klientom mającym ograniczony dostęp do produktów lub usług oferowanych w ramach tego systemu,
- oferowanie produktów lub usług powiązanych z klientem, w przypadku których ryzyko prania pieniędzy oraz finansowania terroryzmu jest ograniczane za pomocą innych czynników, w tym jednostek uczestnictwa funduszy inwestycyjnych otwartych lub specjalistycznych funduszy inwestycyjnych otwartych lub określonych rodzajów pieniądza elektronicznego.
- powiązanie stosunków gospodarczych lub transakcji okazjonalnej z państwem członkowskim Unii Europejskiej, państwem członkowskim Europejskiego Porozumienia o Wolnym Handlu, państwem trzecim określanym przez wiarygodne źródła jako państwo o niskim poziomie korupcji lub innej działalności przestępczej, państwem trzecim, w którym według danych pochodzących z wiarygodnych źródeł obowiązują przepisy dotyczące przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu odpowiadające wymogom wynikającym z przepisów Unii Europejskiej z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu[41].

Z kolei biuro rachunkowe jako instytucja obowiązana nie może zastosować uproszczonych środków bezpieczeństwa finansowego, w przypadku gdy występuje podejrzenie prania pieniędzy lub finansowania terroryzmu, a także wątpliwości co do prawdziwości lub kompletności dotychczas uzyskanych danych identyfikacyjnych klienta.

Stosowanie wzmożonych środków bezpieczeństwa finansowego jest możliwe w przypadkach, w których ocena ryzyka potwierdziła wyższe ryzyko prania pieniędzy oraz finansowania terroryzmu. Katalog sytuacji potencjalnie wyższego ryzyka jest zawarty w art. 43 ust. 2 i jest katalogiem otwartym. Wśród sytuacji uznawanych przez ustawodawcę jako potencjalnie wyższego ryzyka warto wskazać choćby na: nietypową lub nadmiernie złożoną strukturę własnościową klienta, biorąc pod uwagę rodzaj i zakres prowadzonej przez niego działalności gospodarczej[42]. Wzmożone środki bezpieczeństwa finansowego należy też wprowadzić w sytuacji gdy klient korzysta z usług lub produktów sprzyjających anonimowości

[41] Art. 42, ust. 2. u.p.p.p.

[42] Art. 43, ust. 2 pkt 4. u.p.p.p.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

lub utrudniających jego identyfikację, w tym z usługi polegającej na tworzeniu dodatkowych numerów rachunków[43]. Wystąpienie jednak sytuacji przewidzianej w art. 42 u.p.p.p. nie obliguje w sposób automatyczny do stosowania wzmożonych środków bezpieczeństwa finansowego. To ocena ryzyka musi potwierdzić występowanie zdarzeń, które mogą powodować wyższe ryzyko prania pieniędzy i finansowania terroryzmu. Stosunki gospodarcze z podmiotami, które nie zostały wymienione w art. 43 ust. 2 u.p.p.p. również mogą potwierdzić wyższe ryzyko wystąpienia prania pieniędzy i finansowania terroryzmu.

8.6. WEWNĘTRZNA PROCEDURA BIURA RACHUNKOWEGO W ZAKRESIE PRZECIWDZIAŁANIA PRANIU PIENIĘDZY ORAZ FINANSOWANIU TERRORYZMU

Instytucje obowiązane wprowadzają wewnętrzną procedurę w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, zwaną dalej „wewnętrzną procedurą instytucji obowiązanej"[44]. To Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 82005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. UE. L. z 2015 r. nr 141, str. 73 z późn. zm.), gdzie w art. 8 ust 3 nakłada na państwa członkowskie obowiązek zapewnienia posiadania przez podmioty zobowiązane strategii, środków kontroli oraz procedur służących skutecznemu ograniczaniu ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu oraz skutecznemu zarządzaniu tym ryzykiem zidentyfikowanym na poziomie Unii, państwa członkowskiego oraz na poziomie podmiotu zobowiązanego. Wewnętrzna procedura jest dokumentem wewnętrznym każdej instytucji obowiązanej, w której mają zostać doprecyzowane zasady postępowania stosowane w instytucji obowiązanej, w celu właściwego wywiązania się z nałożonych na tę instytucję obowiązków z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Ustawodawca określa i wylicza zasady postępowania jakie instytucja obowiązana powinna zawrzeć w procedurze wewnętrznej. Nie jest to jednak katalog zamknięty, bowiem ustawodawca używa sformułowania, że wewnętrzna procedura instytucji obowiązanej „obejmuje w szczególności", a więc dopuszcza możliwość innych zasad, które będą współtworzyć procedurę wewnętrzną instytucji obowiązanej. Trzeba jednak zaznaczyć, że określenie

[43] Art. 43, ust. 2 pkt 6. u.p.p.p.
[44] Art. 50, ust. 1 u.p.p.p.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

„w szczególności" pociąga za sobą obowiązek stosowania wymienionych w art. 50 ust. 2 u.p.p.p. zasad, które powinny uwzględniać charakter oraz rodzaj i rozmiar prowadzonej działalności instytucji obowiązanej. Wśród zasad, o których mowa, ustawodawca wskazuje, aby procedura wewnętrzna instytucji obowiązanej obejmowała w szczególności określenie:

- czynności lub działań podejmowanych w celu ograniczenia ryzyka prania pieniędzy oraz finansowania terroryzmu,
- zasad rozpoznawania i oceny ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z danymi stosunkami gospodarczymi lub transakcją okazjonalną,
- środków stosowanych w celu właściwego zarządzania rozpoznanym ryzykiem,
- zasad stosowania środków bezpieczeństwa finansowego,
- zasad przechowywania dokumentów oraz informacji,
- zasad wykonywania obowiązków obejmujących przekazywanie Generalnemu Inspektorowi informacji o transakcjach oraz zawiadomieniach,
- zasad upowszechniania wśród pracowników instytucji obowiązanej wiedzy z zakresu przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,
- zasad zgłaszania przez pracowników rzeczywistych lub potencjalnych naruszeń przepisów,
- zasad kontroli wewnętrznej lub nadzoru zgodności działalności instytucji obowiązanej z przepisami o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[45].

Zgodnie natomiast z ust. 3 komentowanego przepisu, wewnętrzna procedura podlega akceptacji przez kadrę kierowniczą wyższego szczebla[46].

8.7. INFORMACJE O TRANSAKCJACH PONADPROGOWYCH W BIURZE RACHUNKOWYM

Instytucje zobowiązane z wyjątkiem instytucji, o których mowa w art. 2 ust. 1 pkt 11, 13–15a i 18 zgodnie z przepisem art. 72 ust. 1 u.p.p.p., przekazują Generalnemu Inspektorowi Informacji Finansowej informacje o przyjętej wpłacie lub dokonanej wypłacie środków pieniężnych o równowartości przekraczającej 15 000 euro, a także o wykonanym transferze środków pieniężnych o równowartości przekra-

[45] Zob. art. 50, ust. 2, pkt 1–9 u.p.p.p.

[46] Szerzej na ten temat: A. Rycerski (w:) *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Warszawa 2020, art. 50.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

czającej 15 000 euro. Instytucje obowiązane przekazują również Generalnemu Inspektorowi informacje o przeprowadzonych transakcjach kupna lub sprzedaży wartości dewizowych, których równowartość przekracza 15 000 euro, albo o pośredniczeniu w przeprowadzeniu takich transakcji[47]. Istotnym w przepisie tego artykułu jest zapis wyłączający instytucje obowiązane, o których mowa w art. 2 ust. 1 pkt 11, 13–15a i 18, z obowiązku przekazywania GIIF informacji o transakcjach nadprogowych. Jedną z wymienionych wśród tych podmiotów instytucji obowiązanych są przedsiębiorcy w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz.U. z 2021 r. poz. 162), których podstawową działalnością gospodarczą jest świadczenie usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego, niebędący innymi instytucjami obowiązanymi. Jak z powyższych zapisów wynika, biura rachunkowe, które nie świadczą usług w zakresie prowadzenia ksiąg rachunkowych, zostały wyłączone z obowiązku raportowania transakcji „ponadprogowych". Oczywiście, osoba fizyczna świadcząca usługi z zakresu prowadzenia ksiąg podatkowych pozostaje nadal przedsiębiorcą i co do zasady na podmiocie wskazanym w przepisie art. 2 ust. 1 pkt 24 u.p.p.p. ciąży na nim obowiązek raportowania transakcji „ponadprogowych" w kontekście bycia instytucją obowiązaną z innego tytułu.

Instytucje obowiązane, stosownie do normy zawartej w art. 74 ust 1 u.p.p.p., „mają obowiązek przekazywania GIIF także informacji o okolicznościach, które uzasadniają podejrzenie popełnienia przestępstwa prania pieniędzy i finansowania terroryzmu"[48]. Należy przyjąć, że za okoliczności, które uzasadniają podejrzenia popełnienia przestępstwa prania pieniędzy i finansowania terroryzmu wskazać trzeba przede wszystkim okoliczności nietypowe, niejasne, wątpliwe, anormalne, niezwykłe czy nadzwyczajne, które polegają na działaniu niespójnym ze znanym i udokumentowanym charakterem działalności klienta lub na występowaniu nietypowych obrotów dla danego rodzaju rachunku, umowy czy kontraktu, które mogą stanowić symptomy uzasadnionego podejrzenia prania pieniędzy[49]. Informacje, jakie powinny znaleźć się w zawiadomieniu zostały enumeratywnie wyliczone w art. 74 ust. 3 pkt 1–8 u.p.p.p. Jak stanowi przepis, w zawiadomieniu podaje się:

[47] Z dniem 31 lipca 2021 r. art. 72, ust. 1 zdanie wstępne zostało zmienione przez art. 1 pkt 44 ustawy z dnia 30 marca 2021 r. (Dz.U. z 2021 r., poz. 815) zmieniającej nin. ustawę z dniem 31 lipca 2021 r.

[48] W. Ługowski (w:) *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Wolters Kluwer, art. 74, Warszawa 2020.

[49] Zob. J.W. Wójcik, *Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Twigger, Warszawa 2002, s. 337; E. Gołębiowska, W. Jasiński, J. Odziomek, J.W. Wójcik, *Zadania instytucji obowiązanych w przeciwdziałaniu praniu pieniędzy. Poradnik dla instytucji obowiązanych*, Wolters Kluwer, Warszawa 2001, s. 33–34; E. Pływaczewski, *Proceder prania pieniędzy i jego implikacje*, LEX, Warszawa 2013.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- dane identyfikacyjne, o których mowa w art. 36 ust. 1, klienta instytucji obowiązanej przekazującej zawiadomienie, czyli dane związane z identyfikacją klienta, takie jak imię i nazwisko, obywatelstwo, nr PESEL, seria i numer dokumentu tożsamości, adres zamieszkania oraz NIP i nazwę (firmę) oraz adres głównego miejsca wykonywania działalności gospodarczej – w przypadku osoby fizycznej, a w przypadku osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej, nazwę (firmę), dane o formie organizacyjnej, adres siedziby lub adres prowadzenia działalności, NIP, a w przypadku braku takiego numeru – państwo rejestracji, rejestr handlowy oraz numer i datę rejestracji, oraz dane identyfikacyjne, o których mowa w pkt 1 lit. a i c u.p.p.p., osobę reprezentującą tę osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej,
- dane identyfikacyjne, o których mowa w art. 36 ust. 1, klienta instytucji obowiązanej przekazującej zawiadomienie,
- rodzaj i wielkość wartości majątkowych oraz miejsce ich przechowywania,
- numer rachunku prowadzonego dla klienta instytucji obowiązanej przekazującej zawiadomienie,
- posiadane informacje, o których mowa w art. 72 ust. 6, w odniesieniu do transakcji lub prób ich przeprowadzenia,
- wskazanie państwa Europejskiego Obszaru Gospodarczego, z którym jest powiązana transakcja, jeżeli została przeprowadzona w ramach działalności transgranicznej,
- posiadane informacje o rozpoznanym ryzyku prania pieniędzy lub finansowania terroryzmu oraz o czynie zabronionym, z którego mogą pochodzić wartości majątkowe,
- uzasadnienie przekazania zawiadomienia.

Zawiadomienie jest przekazywane niezwłocznie, nie później jednak niż w terminie 2 dni roboczych od dnia potwierdzenia przez instytucję obowiązaną podejrzenia[50].

8.8. PODSUMOWANIE

Dla przedsiębiorców, których podstawową działalnością gospodarczą jest świadczenie usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego, obowiązki nałożone przez ustawodawcę mogą stanowić poważny problem. Przede wszystkim zakres płaszczyzn, po których biura rachunkowe się

[50] Zob. art. 74, ust. 2 u.p.p.p.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

poruszają, jest niezwykle obszerny. Mowa tu nie tylko o przepisach prawa bilansowego, podatkowego czy gospodarczego, ale również ubezpieczeń społecznych, prawa pracy, a niejednokrotnie także ochrony środowiska. Biorąc pod uwagę tempo zmian, ale i różnorodność interpretacyjną przepisów, trzeba stwierdzić, że dodatkowe obowiązki z zakresu monitorowania i raportowania zdarzeń związanych z praniem pieniędzy i finansowaniem terroryzmu są zadaniem postrzeganym przez biura rachunkowe jako – *nomen omen* – „ponadprogowe". Czy w związku z powyższym dodanie do treści u.p.p.p. art. 2 ust. 1 pkt 15a było właściwym rozwiązaniem legislacyjnym? Oczywiście z perspektywy samych biur rachunkowych, które do tej pory nie wpisywały się w definicję instytucji obowiązanej, wydaje się rozwiązaniem błędnym lub co najmniej nieprzemyślanym przez ustawodawcę. Jednakże z perspektywy celów, jakie wyznaczają przepisy o praniu pieniędzy i finansowaniu terroryzmu, jest krokiem we właściwą stronę. Należy jednak wskazać, że obowiązki, jakie nakłada u.p.p.p. na instytucje obowiązane w wielu przypadkach stanowią zobowiązanie tych instytucji do działań, które powinny być realizowane przez właściwe służby dysponujące odpowiednimi środkami[51].

[51] M. Szurek, *Pozyskiwanie śladów finansowania terroryzmu i ich przetwarzanie*, Gdańskie Wydawnictwo Oświatowe, Gdańsk 2021.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Radosław Sałata
Wyższa Szkoła Gospodarki Euroregionalnej
w Józefowie

ROZDZIAŁ 9.

OBOWIĄZKI KONTROLNE STAROSTY WOBEC FUNDACJI I STOWARZYSZEŃ W ZWIĄZKU Z USTAWĄ O PRZECIWDZIAŁANIU PRANIU PIENIĘDZY ORAZ FINANSOWANIU TERRORYZMU

9.1. UWAGI WPROWADZAJĄCE

Przepisy nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zasadniczo nie wprowadziły dużej liczby zmian dla organów jednostek samorządu terytorialnego. W dniu 13.07.2018 r. weszła w życie zupełnie nowa ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[1].

Zgodnie z uzasadnieniem do ustawy, głównym celem przyjętych przepisów było m.in. dostosowanie europejskich regulacji AML/CFT do wymogów wynikających ze znowelizowanych zaleceń Financial Action Task Force, a także usprawnienie współpracy oraz wymiany informacji pomiędzy jednostkami analityki finansowej państw członkowskich, jak również wypracowanie spójnej unijnej polityki wobec państw trzecich.

Podmiotami, które zostały zobowiązane do podejmowania określonych czynności, są przede wszystkim szeroko rozumiane instytucje finansowe (instytucje obowiązane). Jednakże przepisy AML/CFT zawierają również obowiązki wobec

[1] Dz.U. z 2018 r., poz. 723.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

innych podmiotów, m.in. wobec jednostek samorządu terytorialnego[2]. Omawiane regulacje prawne dotyczą również organów JST, aczkolwiek zadania tego organu wykonuje jego urząd. Organy JST, obok organów administracji rządowej oraz innych państwowych jednostek organizacyjnych, a także NBP, KNF i NIK, zgodnie z definicją zawartą w art. 2 ust. 2 pkt. 8 ww. ustawy stanowią jednostki współpracujące. W istocie chodzi o współdziałanie z Generalnym Inspektorem Informacji Finansowej, zwanym w ustawie „Generalnym Inspektorem".

Poniżej zostaną przedstawione podstawowe ogólne obowiązki starostwa jako instytucji współpracującej. Do najważniejszych zadań jednostek współpracujących należy opracowanie instrukcji postępowania na wypadek sytuacji podejrzenia popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu. Obowiązek ten wynika z art. 83 ust. 1 ww. ustawy. Co więcej, m.in. organy JST niezwłocznie powiadamiają Generalnego Inspektora o podejrzeniu popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu. W ustawie znalazł się przepis regulujący zakres takiego powiadomienia (83 ust. 2 ww. ustawy).

Celem niniejszego rozdziału jest analiza obowiązków kontrolnych, do których jest zobowiązany starosta wobec fundacji i stowarzyszeń w związku z ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

9.2. USTAWOWY OBOWIĄZEK KONTROLI STOWARZYSZEŃ I FUNDACJI PRZEZ STAROSTĘ

Powszechnie wiadomo, iż omawiane zjawisko określa czynności, których celem jest ukrycie pochodzenia środków finansowych uzyskanych z działalności przestępczej oraz nadania im cech charakterystycznych dla legalnych dochodów. Pranie pieniędzy znacząco wpływa na destabilizację gospodarki, zakłóceń w systemie podatkowym oraz walutowym poszczególnych państw. Proceder ten znacząco narusza zasady uczciwej konkurencji, a także powoduje dysproporcję mechanizmu rynkowego określania parametrów ekonomicznych. Pranie pieniędzy wpływa na korupcję w organach administracji, szczególnie w przypadkach jednostek decyzyjnych w zakresie zakazów odnoszących się do niektórych obszarów działalności gospodarczej. Wiadomym jest, iż poprzez zjawisko omawianego przestępstwa przejmowane są niektóre sektory gospodarki przez grupy przestępcze o charakterze zorganizowanym. Do innych zagrożeń płynących z tego rodzaju nadużyć należy wykorzystywanie działalności instytucji finansowych, co w rezultacie prowadzi do zachwiania stabilności finansowej, jak również strat innych

[2] Infor Pl, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu – nowe procedury*, Infor Pl, 2018.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

podmiotów. Proceder zasadniczo wpływa na korumpowanie pracowników instytucji dokonującej podejrzanego rodzaju transakcji, co w konsekwencji powoduje zwiększenie strat poprzez nieuzasadnione ekonomicznie decyzje oraz nadużycia.

Z uwagi na powyższe konieczne jest zwrócenie uwagi na szczególne obowiązki kontrolne, które ustawodawca powierzył starostom w stosunku do stowarzyszeń i fundacji. W dalszych rozważaniach warto zauważyć, iż przedmiotowy zakres prania pieniędzy wszedł w życie w dniu 13 lipca 2018 r. na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r. poz. 723 z późn. zm.), zwanej dalej ustawą. Ustawa ma na celu dostosowanie polskich przepisów do przepisów dyrektywy 2015/849 oraz znowelizowanych zaleceń FATF (*The Financial Action Tak Force*), a także zwiększenie efektywności krajowego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Ustawa uwzględnia również doświadczenia związane ze stosowaniem przepisów ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (Dz.U. z 2017 r. poz. 1049 z późn. zm.), zwanej dalej: uchyloną ustawą.

Przepis art. 130 ust. 2 ustawy stanowi, że kontrolę wykonywania przez instytucje obowiązane obowiązków w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu w ramach sprawowanego nadzoru wykonują także starostowie:

- na zasadach określonych w ustawie – w odniesieniu do stowarzyszeń,
- na zasadach określonych w ustawie – w odniesieniu do fundacji.

Wobec powyższego zasadne jest przeanalizowanie regulacji dotyczących obowiązku instytucji obowiązanych, które zawarte zostały w nowej ustawie.

Katalog instytucji obowiązanych (art. 2 ustawy). Zmieniony został zakres podmiotowy instytucji obowiązanych objętych przepisami ustawy[3]. Część instytucji została dopisana, część podmiotów straciła status instytucji obowiązanych. Niektóre z podmiotów stają się instytucją obowiązaną po spełnieniu warunków, tj. po przyjęciu (dokonaniu płatności) w gotówce kwoty przekraczającej 10 000 euro (dotyczy to m.in.: fundacji i stowarzyszeń).

Oznacza to, że w chwili przyjęcia lub dokonania płatności w gotówce kwoty powyżej 10 000 euro, fundacja lub stowarzyszenie stają się automatycznie instytucją obowiązaną, **ale tylko w stosunku do klienta, od którego przyjęły gotówkę lub dokonały płatności w gotówce, zarówno w ramach nawiązanych relacji gospodarczych lub w ramach transakcji okazjonalnej**. Nie należy tego obowiązku przenosić na relacje z innymi klientami lub na inne transakcje, które nie zostały przeprowadzone w formie gotówkowej. **Tylko w tym zakresie, tj. tylko**

[3] A. Golonka, *Polskie regulacje karne wobec „szóstej" dyrektywy Anti-Money Laundering*, „Iusnovum" 2021, nr 1, s. 155–168.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

w stosunku do klienta, z którym fundacja lub stowarzyszenie jest związane umową lub transakcją okazjonalną fundacja lub stowarzyszenie powinny rozpoznać ryzyko, zastosować środki bezpieczeństwa finansowego i, jeśli transakcja przekracza kwotę 15 000 euro, przesłać ją do Generalnego Inspektora Informacji Finansowej, zwanego dalej: Generalny Inspektor[4]. Jeśli fundacja lub stowarzyszenie stały się instytucją obowiązaną, powinny wyznaczyć osobę odpowiedzialną za przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu, wprowadzić wewnętrzną procedurę i przeszkolić pracowników realizujących obowiązki wynikające z ustawy. Po zakończeniu okresu trwania relacji z klientem, od którego przyjęła gotówkę, fundacja lub stowarzyszenie przestaje być instytucją obowiązaną.

Obowiązki instytucji obowiązanych – fundacji i stowarzyszeń. Osoby odpowiedzialne (art. 6, 7, 8 i 9 ustawy):

- wyznaczenie kadry kierowniczej wyższego szczebla odpowiedzialnej za wykonywanie obowiązków określonych w ustawie (art. 6 w zw. z art. 2 ust. 2 pkt. 9),
- wyznaczenie spośród członków organu zarządzającego fundacji lub stowarzyszenia osoby odpowiedzialnej za wdrożenie obowiązków określonych w ustawie (art. 7),
- wyznaczenie pracownika zajmującego kierownicze stanowisko w fundacji lub stowarzyszeniu odpowiedzialnego za zapewnienie zgodności działalności fundacji lub stowarzyszenia oraz ich pracowników z przepisami ustawy (art. 8),
- w przypadku instytucji obowiązanych wykonujących działalność jednoosobowo, osobą odpowiedzialną zarówno za wykonywanie, jak i wdrażanie obowiązków określonych w ustawie jest osoba wykonująca tę działalność (art. 9).

Ocena ryzyka instytucji obowiązanych (art. 27 ustawy). Stosownie do art. 27 ustawy fundacje i stowarzyszenia zostały zobowiązane do identyfikowania i oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, odnoszące się do ich działalności. Powinny przy tym uwzględnić czynniki ryzyka dotyczące: klientów, państw lub obszarów geograficznych, produktów, usług, transakcji lub kanałów ich dostaw. Podejmowane przez nie działania powinny ponadto być proporcjonalne do charakteru i wielkości danej fundacji bądź stowarzyszenia. Przy ocenie ryzyka fundacje i stowarzyszenia mogą uwzględniać krajową ocenę ryzyka, jak również sprawozdania Komisji Europejskiej z ponadnarodowej oceny ryzyka prania pieniędzy oraz finansowania terroryzmu.

Ocena ryzyka powinna być sporządzana w postaci papierowej lub elektronicznej i podlegać bieżącej aktualizacji w związku ze zmianami czynników ryzyka, nie rzadziej niż co dwa lata. W razie potrzeby, w szczególności w związku ze zmia-

[4] M. Kędzierski, *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Prokuratura i Prawo" 2021, nr 5, s. 66.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nami czynników ryzyka dotyczących klientów, państw lub obszarów geograficznych, produktów, usług, transakcji lub kanałów ich dostaw albo ocen ryzyka UE lub krajowej oceny ryzyka, aktualizacja powinna następować częściej. Pierwszą ocenę ryzyka, o której mowa w art. 27 ustawy fundacje i stowarzyszenia sporządzają w terminie 6 miesięcy od dnia wejścia w życie ustawy, tj. **do 13 stycznia 2019 r.** Na żądanie Generalnego Inspektora przekazują przygotowane w zakresie swojej właściwości oceny ryzyka oraz inne informacje mogące mieć wpływ na krajową ocenę ryzyka.

Rozpoznanie i ocena ryzyka klienta (art. 33 ustawy). Fundacje i stowarzyszenia zostały zobowiązane do stosowania środków bezpieczeństwa finansowego wobec swoich klientów. W celu stosowania ww. środków zostały zobowiązane do rozpoznania ryzyka prania związanego ze stosunkami gospodarczymi lub z transakcją okazjonalną i oceny poziomu rozpoznanego ryzyka. Przedmiotowa ocena ma zasadniczy wpływ na intensywność stosowania środków bezpieczeństwa finansowego wobec klientów. Fundacje i stowarzyszenia stosownie do art. 33 ust. 3 ustawy „dokumentują rozpoznane ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz jego ocenę, uwzględniając w szczególności czynniki dotyczące:

- rodzaju klienta,
- obszaru geograficznego,
- przeznaczenia rachunku[5],
- rodzaju produktów, usług i sposobów ich dystrybucji,
- poziomu wartości majątkowych deponowanych przez klienta lub wartości przeprowadzonych transakcji,
- celu, regularności lub czasu trwania stosunków gospodarczych.

Stosowanie środków bezpieczeństwa finansowego (art. 34 ustawy). Środki bezpieczeństwa finansowego obejmują:

- identyfikację klienta oraz weryfikację jego tożsamości,
- identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu:
  - weryfikacji jego tożsamości,
  - ustalenia struktury własności i kontroli – w przypadku klienta będącego osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej,
- ocenę stosunków gospodarczych i, stosownie do sytuacji, uzyskanie informacji na temat ich celu i zamierzonego charakteru,
- bieżące monitorowanie stosunków gospodarczych klienta, w tym:
  - analizę transakcji przeprowadzonych w ramach stosunków gospodarczych w celu zapewnienia, że transakcje te są zgodne z wiedzą instytucji obowią-

[5] A. Alińska, *Alternatywne finanse*, Wydawnictwo CeDuWu, Warszawa 2019.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

zanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz zgodne z ryzykiem prania pieniędzy oraz finansowania terroryzmu związanym z tym klientem,
- badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta w przypadkach uzasadnionych okolicznościami,
- zapewnienie, że posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych są na bieżąco aktualizowane.

W sprawie identyfikacji i weryfikacji beneficjenta rzeczywistego klienta należy podjąć uzasadnione środki weryfikacji jego tożsamości, tak aby instytucja obowiązana była przekonana, że wie, kim jest beneficjent rzeczywisty. W przypadku osób prawnych, trustów, przedsiębiorstw, fundacji i podobnych porozumień prawnych należy podjąć uzasadnione środki w celu zrozumienia struktury własności i kontroli klienta. Przy czym – beneficjentem rzeczywistym jest zawsze osoba fizyczna[6].

Obowiązek identyfikacji beneficjenta rzeczywistego klienta ma charakter bezwzględny. Badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta powinno być stosowane wobec klientów, co do których stosuje się wzmożone środki bezpieczeństwa finansowego.

Środki bezpieczeństwa finansowego – o których mowa powyżej – fundacje i stowarzyszenia stosują w następujących przypadkach:
- nawiązania stosunków gospodarczych,
- przeprowadzania transakcji okazjonalnej (transakcja, która nie jest przeprowadzana w ramach stosunków gospodarczych):
  - o równowartości **15 000 euro** lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja czy kilka operacji, które wydają się ze sobą powiązane, lub
  - nie dotyczy fundacji i stowarzyszeń,
- przeprowadzania gotówkowej transakcji okazjonalnej o równowartości **10 000 euro** lub większej, bez względu na to, czy transakcja jest przeprowadzona jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane – w przypadku instytucji obowiązanych, o których mowa w art. 2 ust. 1 pkt. 23 ustawy,
- nie dotyczy fundacji i stowarzyszeń,
- podejrzenia prania pieniędzy lub finansowania terroryzmu[7],
- wątpliwości co do prawdziwości lub kompletności dotychczas uzyskanych danych identyfikacyjnych klienta.

[6] *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu, Komentarz*, red. W. Kapica, Wolters Kluwer, Warszawa 2020.

[7] R. Lizak, *Pranie pieniędzy w prawie polskim na tle europejskim, międzynarodowym i amerykańskim*, C.H. Beck, Warszawa 2018.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Fundacje i stowarzyszenia stosują środki bezpieczeństwa finansowego w odniesieniu do klientów, z którymi utrzymują stosunki gospodarcze, z uwzględnieniem rozpoznanego ryzyka prania pieniędzy oraz finansowania terroryzmu, w szczególności, gdy doszło do zmiany uprzednio ustalonego charakteru lub okoliczności stosunków gospodarczych[8].

Mogą stosować **uproszczone** środki bezpieczeństwa finansowego w przypadkach określonych w art. 43 ustawy lub **wzmożone** środki bezpieczeństwa finansowego (art. 43). Te ostatnie powinny zostać zastosowane w przypadkach wyższego ryzyka prania pieniędzy lub finansowania terroryzmu. Artykuł 43 ustawy zawiera katalog przykładowych czynników wskazujących na wyższe ryzyko prania pieniędzy oraz finansowania terroryzmu.

Stosując środki bezpieczeństwa finansowego fundacje i stowarzyszenia, powinny dostosowywać intensywność stosowania tych środków w zależności od poziomu rozpoznanego ryzyka prania pieniędzy oraz finansowania terroryzmu. Ustawa rozszerza kategorię PEP o osoby zajmujące eksponowane stanowiska polityczne w Polsce, jak i w instytucjach międzynarodowych niezależnie od jego miejsca zamieszkania. W celu ustalenia, czy klient lub beneficjent rzeczywisty jest osobą zajmującą eksponowane stanowisko polityczne, fundacje i stowarzyszenia wdrażają procedury oparte na analizie ryzyka, w tym mogą przyjmować od klienta oświadczenie w formie pisemnej lub w formie dokumentowej, że jest on albo nie jest osobą zajmującą takie stanowisko, składane pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia. Składający oświadczenie jest obowiązany do zawarcia w nim klauzuli następującej treści: „Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia". Klauzula ta zastępuje pouczenie o odpowiedzialności karnej za złożenie fałszywego oświadczenia. Katalog osób rozumianych jako osoby zajmujące eksponowane stanowiska polityczne (PEP) określa art. 2 ust. 2 ustawy.

Bieżąca analiza transakcji. W aktualnym stanie prawnym fundacje i stowarzyszenia nie mają obowiązku przeprowadzania oddzielnej bieżącej analizy transakcji klientów. Analiza transakcji klienta przeprowadzona jest w ramach środków bezpieczeństwa finansowego – bieżącego monitoringu stosunków gospodarczych. Natomiast w stosunku do klientów, wobec których stosuje się wzmożone środki bezpieczeństwa finansowego, fundacje i stowarzyszenia przeprowadzają wzmożoną bieżącą analizę przeprowadzonych z tym klientem transakcji i dokumentują wyniki tej analizy.

Rejestr transakcji. Ustawa znosi obowiązek prowadzenia rejestru transakcji w obecnym kształcie. Oznacza to, że od 13 lipca 2018 r. fundacje i stowarzyszenia nie są już zobowiązane do prowadzenia rejestru transakcji. Jednakże dane zawarte w dotychczas prowadzonym rejestrze muszą być przechowywane przez okres 5 lat,

[8] Ministerstwo Finansów, *Krajowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu*, Warszawa 2019.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

licząc od pierwszego dnia roku następującego po roku, w którym transakcje zostały zarejestrowane. W przypadku likwidacji, połączenia, podziału oraz przekształcenia fundacji i stowarzyszenia, do przechowywania rejestrów i dokumentacji stosuje się odpowiednio przepisy art. 76 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2018 r., poz. 395 z późn. zm.).

Wewnętrzna procedura. Stosownie do art. 50 ustawy fundacje i stowarzyszenia wprowadzają wewnętrzną procedurę w zakresie przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu, która powinna określać zasady postępowania stosowane w fundacji i stowarzyszeniu. Elementy, jakie powinna zwierać wewnętrzna procedura, określa art. 50 ust. 2 pkt. 1–9 ustawy. Wewnętrzna procedura podlega akceptacji przez kadrę kierowniczą wyższego szczebla[9].

Szkolenia (art. 52 ustawy). Ustawa w istotny sposób zmienia dotychczasowy stan prawny dotyczący przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, konieczne jest zaktualizowanie obowiązków szkoleniowych, określonych w art. 52 ustawy. Szkolenia takie mogą zostać przeprowadzone w formie szkolenia zewnętrznego lub wewnętrznego w fundacji lub stowarzyszeniu, jak również poprzez samokształcenie przy wykorzystaniu informacji i komunikatów dostępnych na stronach Generalnego Inspektora.

Obowiązek przekazywania informacji o transakcjach (art. 72, 74 i 89 ustawy). Fundacje i stowarzyszenia, tak jak dotychczas zobowiązane zostały na podstawie art. 72 ust. 1 ustawy do przekazywania do Generalnego Inspektora informacji o tzw. transakcjach ponadprogowych. Zmianie uległy terminy przekazywania tych informacji w terminie (tj. 7 dni od przyjęcia wpłaty lub dokonania wypłaty środków pieniężnych).

Fundacje i stowarzyszenia zobowiązane zostały na podstawie art. 74 ust. 1 ustawy do zawiadamiania Generalnego Inspektora o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu. Przepis przewiduje odejście od konieczności wystąpienia transakcji, której okoliczności wskazują, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, tzw. transakcji podejrzanej, jako przesłanki koniecznej do materializacji obowiązku raportowania (*suspicious transaction report*). Zawiadomienie musi być przekazywane niezwłocznie, nie później jednak niż w terminie 2 dni roboczych od dnia potwierdzenia przez fundację podejrzenia (art. 74 ust. 2 ustawy).

Nowym obowiązkiem dla fundacji i stowarzyszenia jest niezwłoczne zawiadomienie właściwego prokuratora o przypadku powzięcia uzasadnienia podejrzenia, że wartości majątkowe będące przedmiotem transakcji lub zgromadzone na rachunku pochodzą z przestępstwa innego niż przestępstwo prania pieniędzy

[9] M.A. Kędzierski, *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce*, Wydawnictwo Adam Marszałek, Toruń 2019.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

lub finansowania terroryzmu lub z przestępstwa skarbowego, albo mają związek z przestępstwem innym niż przestępstwo[10].

Wstrzymywanie transakcji (rozdz. 8 ustawy). Ustawa wprowadza nowe terminy wstrzymania transakcji, które zostały określone w art. 86 ustawy oraz nowe terminy, w przypadku gdy przekazane zawiadomienie było niemożliwe przed przeprowadzeniem transakcji – art. 90 ustawy[11].

Kontrolowanie instytucji obowiązanych (rozdz. 12 ustawy). Nowe zasady dotyczące kontroli instytucji obowiązanych uregulowane zostały w art. 130–146 rozdz. 12 ustawy. Kontrola, o której mowa w art. 130 ustawy, może być przeprowadzona w zakresie i na zasadach określonych w ustawie przez ww. organ pracowników/kontrolerów (art. 131 i art. 132). Szczegółowy zakres upoważnienia do kontroli określa ustawa w art. 133 ust. 2. Z przeprowadzonej kontroli sporządzany jest protokół pokontrolny (art. 141) oraz wystąpienie pokontrolne zawierające m.in. zalecenia pokontrolne (art. 142).

Kary administracyjne (rozdz. 13). Należy podkreślić, że przepisy ustawy zmieniły zakres obowiązków podlegających sankcji administracyjnej (art. 147 i art. 149), jak również wprowadziły rozbudowany zakres kar administracyjnych i wysokość kar pieniężnych (art. 150). Kary administracyjne na fundacje i stowarzyszenia będące instytucjami obowiązanymi w rozumieniu ustawy, w drodze decyzji administracyjnych nakłada Generalny Inspektor.

9.3. WEWNĘTRZNE PROCEDURY AML W STAROSTWIE POWIATOWYM

Na podstawie art. 32 ust. 1 ustawy z dnia 5 czerwca marca 1998 r. o samorządzie powiatowym (tj. Dz.U. z 2020 r., poz. 920, z 2021 r. poz. 1038), art. 2 ust. 2 pkt. 8 i art. 83 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2021 r., poz. 1132) zarząd powiatu powinien podjąć uchwałę w sprawie wprowadzenia instrukcji dotyczącej AML.[12] Instrukcja powinna określić zasady postępowania i odpowiedzialności osób za realizację przepisów ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

[10] W. Kapica, J. Grynfelder, W. Ługowski, T. Mierzwiński, R. Obczyński, A. Otto, E. Patsiotos, Z. Piotrowska, A. Rycerski, J. Stolarczyk, *Przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu komentarze praktyczne*, Wolters Kluwer, Warszawa 2020.

[11] J. Rajewska, M. Strzelecka, *Praktyczne aspekty stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień*, Deloitte 2020.

[12] P. Walczak, *Dokumentacja wewnętrzna w jednostkach sektora finansów publicznych*, C.H. Beck, Warszawa 2020.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

W zależności od schematu organizacyjnego JST w instrukcji wskazać należy koordynatora, który w imieniu starosty będzie koordynatorem ds. współpracy z GIIF. W praktyce dość często przyjmuje się, że najlepszym koordynatorem z uwagi na zakres czynności będzie skarbnik powiatu. Następnie instrukcja powinna zobowiązywać pracowników starostwa powiatowego do zapoznania się z treścią instrukcji i podpisania oświadczenia o przyjęciu do wiadomości według określonego wzoru.

Pracownicy starostwa powiatowego w trakcie wykonywania obowiązków służbowych zobowiązani są do zwracania szczególnej uwagi na transakcje, umowy, zachowania nietypowe opisane szczegółowo w instrukcji, z których może wynikać podejrzenie popełnienia przestępstw prania pieniędzy i finansowania terroryzmu[13].

Pracownik powiatowy na każdym z odcinków pracy, w przypadku powzięcia przekonania, że identyfikuje nietypowe zdarzenie, z którego może wynikać podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu jest zobowiązanych do:

- sporządzenia kopii dokumentów dotyczących transakcji, co do których zachodzi podejrzenie, że mają one związek z popełnieniem przestępstwa, o którym mowa w art. 165a lub art. 299 Kodeksu karnego,
- zebrania dostępnych informacji o osobach przeprowadzających te transakcje,
- sporządzenia notatki służbowej zawierającej opis transakcji wraz z uzasadnieniem, iż zachodzą okoliczności wskazane w art. 83 ww. ustawy,
- przygotowania projektu powiadomienia GIIF i przekazania go Koordynatorowi ds. współpracy z GIIF.

Koordynator ds. współpracy z GIIF w granicach kompetencji ustawowych przekaże stosowne informacje do GIIF[14].

W dość powszechnej praktyce, instrukcje uchwalane przez JST zawierają wskazania, aby pracownicy zwracali szczególną uwagę na:

- transakcje nietypowe związane z nabyciem majątku komunalnego,
- umowy i transakcje związane z wykonywaniem przez inne podmioty zadań publicznych w JST, realizowane na warunkach odbiegających od istniejących standardów,
- nietypowe zachowania i czynności podejmowane przez uczestników postępowania o udzielenie zamówienia publicznego, polegające m.in. na oferowaniu przez nich warunków wykonywania zamówienia w sposób rażąco odbiegających od oferowanych przez innych oferentów,

[13] K. Kocoń, *Prawnopodatkowe aspekty pozyskiwania kapitału w ramach finasowania społecznościowego przez mikro- i małe przedsiębiorstwa*, „Finanse, Rynki Finansowe, Ubezpieczenia" 2017, nr 4 (88), cz. 2, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2020.

[14] K. Grabowska, *MK Monitor księgowego, wydanie specjalne. Przeciwdziałanie praniu brudnych pieniędzy oraz finansowaniu terroryzmu*, Inforlex, Warszawa 2019, s. 80.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- udział kontrolowanych jednostek i innych podmiotów w nietypowych przedsięwzięciach, szczególnie finansowanych z udziałem kapitału zagranicznego,
- dokonywanie wpłaty znacznych kwot gotówkowych (np. tytułem zapłaty za nabyte mienie),
- dokonywanie wpłaty należności w ratach (kilkakrotnie), w tym samym dniu,
- przypadki dokonywania nadpłat (np. podatków i innych opłat) lub wpłat nienależnych jednostce i ewentualnego ich wycofania.

W dalszych rozważaniach warto zauważyć, iż przedmiotowy zakres prania pieniędzy nie stanowi tylko gotówka, ale zróżnicowane pod względem rodzaju składniki majątku, których pochodzenie wynika z działalności przestępczej bądź ich przeznaczenie ma uskutecznić realizację wspomnianej działalności. Zatem przedmiot prania pieniędzy stanowi gotówka, pieniądz depozytowy, kredytowy jak również odrębne wartości majątku, których pochodzenie jest nielegalne i mogą zostać przeznaczone w celu realizacji bądź przygotowania działalności przestępczej.

Jednostka analityki finansowej stanowi centralną, państwową agencję, odpowiedzialną za otrzymywanie (oraz, jeśli to dozwolone, wnioskowanie), analizę i przekazywanie odpowiednim organom ujawnionych informacji finansowych:

i) dotyczących podejrzanych dochodów i potencjalnego finansowania terroryzmu lub

ii) wymaganych przez krajowe prawodawstwo lub przepisy, w celu zwalczania prania pieniędzy i finansowania terroryzmu – na podstawie art. 1 pkt. f Konwencji Rady Europy z dnia 16 maja 2005 r. o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu (Dz.U. z 2008 r., nr 165, poz. 1028).

Wiadomym jest, iż system przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu tworzą w Polsce GIIF oraz instytucje obowiązane, w skład których wchodzą podmioty z sektora finansowego, jak i niefinansowego, oferujące wiele usług bądź produktów mogących stanowić wbrew ich przeznaczeniu narzędzie do prania pieniędzy lub finansowania terroryzmu. Jak również jednostki współpracujące, w skład których wchodzą organy administracji rządowej, organy jednostek samorządu terytorialnego, inne państwowe jednostki organizacyjne, jak również Narodowy Bank Polski (NBP), Komisja Nadzoru Finansowego (KNF) i Najwyższa Izba Kontroli (NIK).

Postanowienia zawarte w ustawie jasno wskazują liczne obowiązki GIIF, instytucji obowiązanych, jak również instytucji współpracujących, uwzględniając znaczenie obszaru współpracy oraz przepływu informacji.

Zasadniczą rolą instytucji obowiązanych jest rozpoznanie oraz ocena ryzyko prania pieniędzy i finansowania terroryzmu mające związek ze relacjami o charakterze gospodarczym zawieranymi z kontrahentami bądź wynikające z transakcji okazjonalnych realizowanymi przez wspomniane podmioty. Poprzez analizę ryzyka

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

oraz jego ocenę wdrażają środki bezpieczeństwa finansowego, których zasadniczą funkcję stanowi przede wszystkim pozyskanie informacji na temat klientów, jak również sprecyzowanie celu, dla którego korzystają oni z usług i produktów oferowanych przez instytucje obowiązane[15].

Regulacje określone w ustawie odnoszą się do organów jednostek samorządów terytorialnych, jednak zadania tego organu wykonuje urząd właściwy. Zgodnie z definicją zawartą w omawianej ustawie Narodowy Bank Polski, Komisja Nadzoru Finansowego oraz Najwyższa Izba Kontroli, organy administracji rządowej, jak również organy jednostek samorządów terytorialnych stanowią ogół jednostek współpracujących. Omawiany zakres współpracy opiera się najczęściej na współdziałaniu z Generalnym Inspektorem Informacji Finansowej.

Poniżej zostaną przedstawione podstawowe, ogólne obowiązki instytucji współpracujących, określone przepisami. Do obowiązków organów jednostek samorządu terytorialnego w kontekście zmiany ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu należy opracowanie instrukcji postępowania na wypadek sytuacji podejrzenia popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu. Ponadto, jak zostało wspomniane, organy jednostek samorządu terytorialnego mają w obowiązku zawiadomić w trybie niezwłocznym Generalnego Inspektora o podejrzeniu popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu. Omawiane powiadomienie powinno zawierać posiadane dane osób fizycznych, osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej, pozostających w związku z okolicznościami mogącymi wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, które jednoznacznie identyfikują daną osobę fizyczną lub prawną, w dalszej części opis okoliczności, jak również uzasadnienie przekazania powiadomienia.

Istotnym aspektem współpracy jest udostępnianie dokumentów lub posiadanych informacji przez organy samorządów terytorialnych na wniosek Generalnego Inspektora[16]. We wniosku Generalny Inspektor może wskazać termin oraz formę ich przekazania lub udostępnienia.

Współpraca organów JST z Generalnym Inspektorem może również dotyczyć konieczności przekazania dokumentów sądom i prokuratorom na potrzeby postępowania karnego w przypadku, gdy żądane przez te organy informacje nie znajdują się w posiadaniu Generalnego Inspektora.

Wiadomym jest, że realizacja wspomnianych zadań jednostek współpracujących występować może tylko wówczas, gdy zaistnieje podstawa, czyli określone zdarzenie. Ponadto regulacje ustawowe wskazują także na czynności wykonywane z określoną częstotliwością. Do takich zadań należy zaliczyć współudział w opra-

[15] M. Capiga, *Bezpieczeństwo instytucji finansowych jako instytucji Obowiązanych w systemie przeciwdziałania praniu pieniędzy*, „Studia Ekonomiczne" 2014, nr 171, s. 120–131.

[16] M. Kędzierski, *Współpraca Agencji Bezpieczeństwa Wewnętrznego*..., s. 134 i n.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

cowaniu krajowej oceny ryzyka prania pieniędzy oraz finansowania terroryzmu, jak również przekazanie Generalnemu Inspektorowi pozyskanych informacji lub dokumentów mogących wpływać na krajową ocenę ryzyka. Przekazanie tych informacji może nastąpić z urzędu lub na żądanie Generalnego Inspektora.

W dalszym etapie Generalny Inspektor na podstawie analizy ryzyka opracowuje procedury przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. W projekcie uwzględnione mogą zostać również zalecenia, które odnosić się będą do organów jednostek samorządów terytorialnych.

Zatem jednostki współpracujące przekazują do Generalnego Inspektora informacje o sposobie realizacji zaleceń zawartych w ww. wspomnianych procedurach, co istotne w przypadku jednostek współpracujących przekazanie informacji odbywa się co najmniej raz na 6 miesięcy od dnia jej ogłoszenia w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".

Z omówionych wyżej obowiązków organów jednostek samorządów terytorialnych można wywnioskować, iż obszar współpracy z Generalnym Inspektorem, polegający na przekazywaniu dokumentów i informacji nie stanowi nowego zakresu obowiązków, nowość w funkcjonowaniu organów gminnych stanowi fakt współpracy w konstruowaniu analizy ryzyka oraz procedur przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

9.4. PODSUMOWANIE

Reasumując, organy jednostek samorządu terytorialnego są wskazane, jako jednostki współpracujące w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Z uwagi na powyższe zapisy zawarte w przepisach ustawowych nakładają na nie wiele powinności, które należy realizować, aby w sposób poprawny wywiązywać się z nałożonych ustawą zadań.

Zjawisko prania środków finansowych stanowi ścisły związek z działalnością zorganizowanych grup przestępczych, z uwagi na co proces eliminacji tego procederu jest mało efektywny i trudny do przeprowadzenia. Niejednokrotnie siatka powiązań grup przestępczych sięga skali międzynarodowej, co również wpływa na jakość przeciwdziałania tego rodzaju przestępstwom. Jak powszechnie wiadomo rozwój technologii informatycznych umożliwia grupom przestępczym sprawne przeprowadzanie transakcji finansowych w skali międzynarodowej. Wspomniane elementy wskazują na konieczność współpracy oraz funkcjonowania właściwych instytucji oraz organizacji w celu efektywnego procesu zwalczania omawianego procederu[17].

[17] W. Kenton, M. Jomes, *Shell Corporation*, 24 października 2020.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Jeżeli zaś mowa o jednostkach samorządu terytorialnego, możliwe jest występowanie omawianej problematyki w obszarach związanych z umowami oraz transakcjami wynikającymi z realizacji przez inne podmioty zadań publicznych, wszelakich transakcji mających związek z nabywaniem mienia komunalnego, realizacji zadań wspólnych jednostek samorządu terytorialnego z kapitałem prywatnym. Zagrożony jest również obszar zamówień publicznych, w szczególności ofert realizacji, znacząco odbiegający od przyjętych standardów. Wątpliwości w tym zakresie budzi również udział jednostek w przedsięwzięciach o charakterze nietypowym w szczególności z udziałem kapitału obcego, wszelakie nadpłaty podatków, uzyskiwanie pożyczek od podmiotów niewiadomego pochodzenia, wykup należności komunalnych. Wspomniane wyżej obszary zagrożeń nie wykazują stabilizacji z uwagi na nieustannie zachodzące modyfikacje, a także występowanie zupełnie nowych.

Problematyka prania środków finansowych jest zjawiskiem powszechnym, i stanowi jedno z najpoważniejszych przestępstw gospodarczych dzisiejszego świata. Jak już zostało wspomniane, ściśle odnosi się do działalności zorganizowanych grup przestępczych. Proceder ukrywania środków pieniężnych niewiadomego pochodzenia w ostatnich latach rozrasta się wywierając znaczący wpływ na światową gospodarkę oraz międzynarodowy system finansowy. Wartość dochodów pochodzących z nielegalnych procederów w skali roku sięgać może nawet 5% globalnego PKB. Jak zauważono, organizacje przestępcze wprowadzają do obrotu finansowego środki nielegalnego pochodzenia poprzez nieustannie postępujący proces rozwoju w zakresie technologicznym, jak również globalizacji. Z uwagi na swoistą swobodę w przepływie kapitału, zróżnicowanych możliwościach technologicznych, a także poprzez dowolność zakresu instrumentów finansowych procedują wiele wielowymiarowych transakcji, mających na celu ukrycie faktycznych źródeł przychodów. Warto zauważyć, iż narzędzie w podejmowaniu działań przestępczych we wskazanym zakresie stanowi swoboda przepływu zarówno osób, towarów, usług i środków finansowych dyktowana jednolitością rynku wewnętrznego Unii Europejskiej[18].

Reasumując, zjawisko, jakie stanowi pranie pieniędzy, prowadzi do destabilizacji funkcjonowania rynku, zachwiania bezpieczeństwa finansowego określonych sektorów gospodarki, które to w sposób pośredni bądź bezpośredni zaangażowane są w omawiany proceder. Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu ma chronić system finansowy przed tymi wspomnianymi zagrożeniami. Nałożyła ona nowe obowiązki również na jednostki samorządów terytorialnych. Niestety, obok spółek prawa handlowego, stowarzyszenia i fundacje są formami prawnymi potencjalnie narażonymi na wykorzystanie do procederu prania brudnych pieniędzy. Konieczność identyfikacji, jak również rejestracji transakcji podejrzanych wywiera poniekąd na jednostkach samorządu terytorial-

[18] R. Lizak, *op. cit*.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nego oraz jednostkach organizacyjnych presję poszerzania swojej wiedzy z tego zakresu, jak również do wykonywania dodatkowych czynności w sytuacji podejrzenia popełnienia przestępstwa.

Podjęta w tym rozdziale problematyka obowiązków starostwa powiatowego wobec fundacji i stowarzyszeń oraz współpraca z Generalnym Inspektorem, stanowi częściowe wyczerpanie założonego celu. Uwidaczniają się kolejne powiązane zagadnienia, jak współpraca starostwa powiatowego przy tworzeniu krajowej oceny ryzyka oraz strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. To wymaga podjęcia dalszych badań, które autor planuje.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Anna Samrau
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 10.

NARZĘDZIA ORGANÓW PAŃSTWOWYCH I PODATKOWYCH W WALCE Z PRANIEM PIENIĘDZY

10.1. UWAGI WPROWADZAJĄCE

Sposoby wyłudzeń i różne bardzo wymyślne techniki prania pieniędzy powodują, że organy państwowe muszą wprowadzać coraz to nowe sposoby radzenia sobie z tymi procedurami. Priorytetem stała się prewencja. Lepiej nie dopuścić do prania pieniędzy niż karać za samo pranie. Samo pranie pieniądza polega na uzyskaniu korzyści majątkowych z wprowadzonego do obrotu pieniądza pochodzącego z nieczystej transakcji. Na rynku finansowym pojawiły się ogromne ilości pieniędzy pochodzących z nielegalnych źródeł. Sprawiło to, że organy państwowe na całym świecie zmuszone zostały do analizy tego zjawiska i podjęcia walki z nim. W art. 7 Konwencji Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej wskazano, że strony zapewniają, aby organy administracyjne (regulacyjne, ścigania, sądowe) miały możliwość współpracy oraz wymiany informacji na szczeblu krajowym, jak i międzynarodowym. Do gromadzenia informacji oraz rozpowszechniania informacji o próbie prania pieniędzy mają służyć powołane jednostki informacji finansowej. Walka z procederem prania brudnych pieniędzy jest ważna, gdyż ma negatywny wpływ na ekonomię państwa. W Warszawie sporządzona w dniu 16 maja 2005 r.[1] Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu uznała za potrzebę powołania JAF. JAF

[1] Dz.U. z 2008 r., nr 165, poz. 1028.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

to jednostka analityki finansowej, jest centralną i państwową agencją wspomagająca pracę GIIF.

Wydawać by się mogło, że problematyka prania pieniędzy to nie problem krajów należących do Unii Europejskiej, lecz raczej problem państw trzecich. Nic bardziej mylnego. Afery finansowe na Litwie czy w Estonii ukazały, jak Rosja wykorzystuje sektory bankowe tych państw, prowadząc podejrzane transakcje bankowe. Jak już wspomniano wcześniej, każde państwo, aby skutecznie poradzić sobie z tym nielegalnym procederem, powinno podjąć dwa działania, zapobiegać i zwalczać. Aby zapobiegać, należy wprowadzić regulacje prawne i określić funkcje, jakie powinny pełnić organy państwowe i instytucje obowiązane. Organy te mają na celu przeciwdziałać praniu brudnych pieniędzy. Jeśli jednak dojdzie do czynu zabronionego, to organy państwowe mają wiele uprawnień do zwalczania tych procedur. Przestępstwo prania brudnych pieniędzy i jego zwalczanie dotyczy nie tylko instytucji państwowych czy podmiotów obowiązanych, ale także każdego obywatela. Każdego roku na świecie prane są ogromne sumy pieniądzy.

Podstawowym założeniem niniejszego rozdziału jest teza, według której przyjęte przez Polskę rozwiązania prawne i instytucjonalne przeciwdziałania praniu brudnych pieniędzy są niewystarczające. Celem pracy jest analiza i ocena wymienionych wyżej rozwiązań.

Polski JAF posiada uprawnienia tylko administracyjno-kontrolne. Nie ma możliwości prowadzenia śledztw czy czynności operacyjno-rozpoznawczych. JAF usytuowany jest w strukturze Ministerstwa Finansów współpracując z innymi podmiotami administracyjnymi. Instytucje obowiązane mają obowiązek współpracować z jednostką informacji finansowej, która to weryfikuje przesłane informacje pod kątem możliwości próby prania brudnych pieniędzy. Wiele podmiotów jest zaangażowanych w walkę z terroryzmem tego rodzaju, powołano m.in. Centrum Antyterrorystyczne w ABW (CAT)[2].

Podstawowym jednak organem do walki z praniem brudnych pieniędzy, organem państwowym właściwym dla spraw w zakresie przeciwdziałania finansowaniu terroryzmu jest minister właściwy do spraw instytucji finansowych jako naczelny organ informacji finansowej oraz Generalny Inspektor Informacji Finansowej. Polska przyjęła trzy poziomy sposobów walki z terroryzmem: strategiczny, operacyjny i taktyczny. Strategiczny realizowany jest przez Prezesa Rady Ministrów, Radę Ministrów oraz Międzynarodowy Zespół ds. Zagrożeń Terrorystycznych. Operacyjny realizowany jest przez Centrum Antyterrorystyczne działające w ramach Agencji Bezpieczeństwa Wewnętrznego dalej ABW. Dalej właśnie m.in. ABW, Policja czy Straż Graniczna wykorzystują model strategiczny do walki z przestępstwem prania brudnych pieniędzy.

[2] M. Obuchowicz, *Pięć lat funkcjonowania Centrum Antyterrorystycznego ABW (2008–2013*), „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 275.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Na oficjalnej stronie Ministerstwa Finansów[3] znaleźć można informację, że system do walki z finansowaniem terroryzmu i praniem brudnych pieniędzy w Polsce tworzą: GIIF, jednostki obowiązane oraz jednostki współpracujące. GIFF jest postrzegany głównie jako baza danych, i tutaj również nasuwa się stwierdzenie, że powinno się mu rolę rozszerzyć. Powinien być organem współpracującym z CBA, ABW, Policją, SWW, SKW i innymi, dla których to GIFF jest tylko bazą danych, bazą o przeprowadzonych transakcjach.

Należy tu wspomnieć, że wprowadzenie obowiązku raportowania do GIFF transakcji powyżej kwoty 15 000,00 euro jest jednym z narzędzi przeciwdziałania praniu brudnych pieniędzy[4].

10.2. ORGANY INSTYTUCJONALNE ZAJMUJĄCE SIĘ PRZECIWDZIAŁANIEM PRANIU BRUDNYCH PIENIĘDZY

Instytucje obowiązane, jak również jednostki współpracujące mają obowiązek raportowania każdej transakcji podejrzanej do polskiej jednostki analityki finansowej, tj. do Departamentu Informacji Finansowej. Jednostka ta jest nadzorowana bezpośrednio przez Generalny Inspektorat Informacji Finansowej. W Ministerstwie Finansów funkcjonuje organ PJAF, który dokonuje weryfikacji danych zawartych w raportach, zbiera materiał dowodowy oraz, jeśli jest taka zasadność, podejmuje działania zmierzające do postawienia aktu oskarżenia podejrzanym osobom. Wymiana informacji dokonuje się na szczeblu polskim i międzynarodowym. Wymiana ta dokonuje się na podstawie aż 68 porozumień dwustronnych oraz na podstawie decyzji Rady UE 2000/642/JHA z dnia 17 października 2000 r. w sprawie zasad współpracy pomiędzy jednostkami analityki finansowej państw członkowskich w odniesieniu do wymiany informacji. PJAF dla poprawy jakości działającego sytemu i tworzenia nowych rozwiązań, uczestniczy też w pracach innych organizacji takich, jak: Grupy Egmont ds. Jednostek Wywiadu Finansowego, Komitetu Kontaktowego ds. Zapobiegania Praniu Pieniędzy, Specjalnego Komitetu Ekspertów Rady Europy ds. Oceny Środków Przeciwdziałania Praniu Pieniędzy w Krajach Europy Środkowej i Wschodniej – Moneyval, Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy – FATF, Grupy Euro-Azjatyckiej – EAG, Grupy Zadaniowej ds. Zwalczania Przestępczości Zorganizowanej w regionie Morza Bałtyckiego – BALTCOM.

[3] *Przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmowi*, https://www.gov.pl/web/finanse/przeciwdzialanie-praniu-pieniedzy-i-finansowaniu-terroryzmu (data dostępu: 3 września 2021).

[4] M. Smolak, *Formy zwalczania procederu prania brudnych pieniędzy*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 13, s. 294.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Około 80% czynności związanych z procedurą przestępczą w zakresie prania brudnych pieniędzy ma charakter międzynarodowy. Inicjatywy międzynarodowe mają też na celu wyzbycie się sytuacji, gdzie w jednym państwie pranie brudnych pieniędzy jest zabronione, a w innym nie[5].

J.W. Wójcik uważa, że z punktu widzenia systemowego organy winny rozpoznać rodzaje grup terrorystycznych, wszystkich ich członków i powiązań. Powinny również wyeliminować przepływ pieniędzy przez Polskę w ramach prania brudnych pieniędzy[6].

A. Fijałkowska natomiast wymienia na szczeblu krajowym podmioty odpowiedzialne za przeciwdziałanie praniu brudnych pieniędzy, podmioty wymienione w ustawie ATL z dnia 16 listopada 2000 r. nowelizowanej kilkakrotnie, czyli Generalnego Inspektora Informacji Finansowej, instytucje obowiązane, jak również: prokuraturę, ABW i jednostki inne, podległe ministrowi właściwemu do spraw wewnętrznych[7].

Warto wspomnieć art. 3 ust. 1 pkt 5 ustawy o przeciwdziałaniu, zawiera zapis, że przepisy niniejszego aktu nie naruszają przepisów ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[8]. Agencje te również zwalczają pranie brudnych pieniędzy i finansowanie terroryzmu. Również inne podmioty, jak ABW czy AW mogą realizować zadania w tym zakresie.

Rada Ministrów uchwałą z dnia 19 kwietnia 2021 r. przyjęła strategię przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu[9]. Został opracowany KSPPPFT, tj. krajowy system przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Jest systemem złożonym z wielu połączonych elementów.

Rysunek 1. Schemat KSPPPFT

Źródło: opracowanie własne na podstawie raportu strategicznego Monitor Polski poz. 435.

[5] J.W. Wójcik, *Pranie pieniędzy. Kryminologiczna ocena transakcji w procesie prania pieniędzy*, Twigger, Warszawa 2002, s. 133.

[6] J.W. Wójcik, *Przeciwdziałanie finansowaniu terroryzmu*, Wolters Kluwer, Warszawa 2007, s. 70.

[7] A. Fijałkowska, *Pranie pieniędzy oraz finansowanie terroryzmu jako współczesne zagrożenia bezpieczeństwa powszechnego i obrotu gospodarczego*, Wyższa Szkoła Bezpieczeństwa w Poznaniu, Poznań 2014, s. 181–182.

[8] Dz.U. z 2010 r., nr 29, poz. 154, z późn. zm.

[9] Uchwała nr 50 Rady Ministrów z dnia 19 kwietnia 2021 r. w sprawie przyjęcia strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (M.P. z 2021 r., poz. 435).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Jednostki zobowiązane podzielone są na różne kategorie, przy czym wiele z nich nie podlega odpowiedniemu nadzorowi właściwych organów nadzorczych. Wydaje się że nadzór nad jednostkami obowiązanymi jest szalenie istotny w walce z procederem prania brudnych pieniędzy i finansowania terroryzmu. Zgodnie z art. 130 ustawy o przeciwdziałaniu uprawnieni do takiej kontroli są oprócz GIIF:

- Prezes NBP w odniesieniu do podmiotów prowadzących działalność kantorową w rozumieniu tej ustawy,
- KNF w odniesieniu do instytucji obowiązanych przez nią nadzorowanych,
- Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa w odniesieniu do spółdzielczych kas oszczędnościowo-kredytowych,
- prezesi sądów apelacyjnych w odniesieniu do notariuszy,
- naczelnicy urzędów celno-skarbowych w odniesieniu do instytucji obowiązanych kontrolowanych przez te organy,
- wojewodowie lub starostowie w odniesieniu do stowarzyszeń,
- ministrowie lub starostowie w odniesieniu do fundacji.

Tylko naczelnicy urzędów skarbowych (obok GIFF) mogą kontrolować instytucje obowiązane z różnych kategorii podmiotów.

Dodać należy jeszcze, że organem administracji finansowej (FIU) jest minister właściwy do spraw instytucji finansowych jako organ naczelny informacji finansowej oraz Generalny Inspektor Informacji Finansowej. Minister Finansów jest odpowiedzialny za realizację przepisów ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmowi[10].

10.2.1. GENERALNY INSPEKTOR INFORMACJI FINANSOWEJ

GIIF, czyli Generalny Inspektor Informacji Finansowej ma za zadanie współpracować z jednostkami obowiązanymi i współpracującymi. Pośrednio również współpracuje z organami ścigania. Jednostką współpracującą i wyodrębnioną w strukturze Ministerstwa Finansów jest Departament Informacji Finansowej (DIF).

Art. 72[11] ustawy o przeciwdziałaniu stanowi, iż jednym z podstawowych zadań GIFF jest analiza informacji o transakcjach, w szczególności tych ponadprogowych, i reagowanie na jakiekolwiek informacje o podejrzanych transakcjach. GIFF ma możliwość swobodnego śledzenia transakcji pieniężnych. Ustawa nakłada zakres podmiotowy i przedmiotowy obowiązku raportowania o transakcjach ponadprogo-

[10] Uchwała nr 50 Rady Ministrów z 19 kwietnia 2021 r., Monitor Polski, poz. 435.

[11] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2021 r., poz. 1132 z późn. zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wych do GIIF. Ponadprogowe, czyli przekraczające równowartość 15 000,00 euro oraz transakcje bezgotówkowe o takiej wartości.

Instytucje obowiązane przekazują do GIFF w szczególności informacje o:

- przyjęciu wpłat lub dokonanych wypłatach środków pieniężnych o równowartości przekraczającej 15 000,00 euro lub
- wykonanym transferze środków pieniężnych o równowartości przekraczającej 15 000,00 euro, w tym również:
  - transferu środków pieniężnych spoza Polski na rzecz odbiorcy, którego dostawcą usług płatniczych jest instytucja obowiązana,
  - informacji o przeprowadzonej transakcji kupna lub sprzedaży wartości dewizowych, których równowartość przekracza 15 000 euro (albo już o samym pośredniczeniu w takiej transakcji) – w każdym przypadku z uwzględnieniem określonych w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wyjątków.

Ustawa przewiduje również wyjątki od przymusu składania raportów, wyjątkami są:

- transfery środków pieniężnych pomiędzy rachunkiem płatniczym i rachunkiem lokaty terminowej, które należą do tego samego klienta w tej samej instytucji obowiązanej,
- krajowy transfer środków pieniężnych z innej instytucji obowiązanej,
- transakcje związane z gospodarką własną instytucji obowiązanej, które zostały przeprowadzone przez instytucję obowiązaną we własnym imieniu i na własną rzecz, w tym transakcje zawarte na rynku międzybankowym,
- transakcje przeprowadzone w imieniu lub na rzecz jednostek sektora finansów publicznych, o których mowa w art. 9 u.f.p.,
- transakcje przeprowadzone przez bank zrzeszający banki spółdzielcze, jeżeli informacja o transakcji została przekazana przez zrzeszony bank spółdzielczy,
- przewłaszczenia na zabezpieczenie wartości majątkowych wykonane na czas trwania umowy przewłaszczenia z instytucją obowiązaną[12].

W myśl tych przepisów rodzi się pytanie, czy przekazywanie między rachunkami na kontach biur maklerskich czy domu maklerskiego środków powyżej wartości ponadprogowej rodzi obowiązek raportowania. W komentarzu do ustawy W. Kapica stwierdza, że „transfery środków pieniężnych realizowane przez biuro maklerskie czy dom maklerski pomiędzy rachunkami pieniężnymi prowadzonymi

[12] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2021 r., poz. 1132 z późn. zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

na podstawie ustawy o obrocie instrumentami finansowymi podlegają raportowaniu na podstawie art. 72 ust. 1 pkt.2 ustawy”[13].

W odniesieniu do raportowania o wpłacie lub wypłacie środków pieniężnych o równowartości przekraczającej 15 000,00 euro, GIFF wydał komunikat publiczny[14], w którym wyjaśnia, że obowiązek ten dotyczy wyłączenie transakcji przyjętej lub wydanej w gotówce do kasy lub rachunek bankowy prowadzony przez raportującą instytucję obowiązaną.

Ma to miejsce wyłącznie w sytuacji:

- gdy klient otrzymuje od instytucji obowiązanej w formie gotówki środki pieniężne, które były zdeponowane na rachunku płatniczym prowadzonym przez dokonującą wypłaty instytucję obowiązaną (będącą dostawcą usług płatniczych), bez względu na to, czy rachunek płatniczy jest prowadzony na rzecz klienta odbierającego wypłacane środki czy na rzecz innego podmiotu (który upoważnił osobę odbierającego wypłacane środki), lub
- gdy klient otrzymuje z kasy instytucji obowiązanej środki pieniężne w formie gotówki.

W komunikacie tym też GIFF wyjaśnia, że transakcje opłacone kartą płatniczą nie są wpłatą gotówkową, natomiast płatność mieszana częściowo kartą i częściowo gotówką powoduje sprawdzenie, czy istnieje obowiązek raportowania takiej transakcji.

Do przekazywania informacji do GIIF zobowiązane są wszystkie instytucje zobowiązane, z wyjątkiem niektórych wymienionych w ustawie, tj. wskazanych w:

- art. 2 ust. 1 pkt 11 (prowadzący działalność kantorową i niektóre inne podmioty prowadzące zbliżoną działalność) – natomiast przedmiotowe podmioty prowadzące działalność kantorową lub niektóre podmioty prowadzące zbliżoną działalność zobowiązane są do raportowania transakcji kupna lub sprzedaży wartości dewizowych (czyli wymiany walut) na podstawie art. 72 ust. 3 ustawy w przypadku, jeśli równowartość transakcji przekracza kwotę 15 000 euro,
- art. 2 ust. 1 pkt 13 (notariusze – w zakresie czynności dokonywanych w formie aktu notarialnego obejmującego określone czynności prawne),
- art. 2 ust. 1 pkt 14 (adwokaci, radcowie prawni, prawnicy zagraniczni i doradcy podatkowi – co do określonego zakresu świadczonej pomocy prawnej lub doradztwa podatkowego),

[13] W. Ługowski (w:) *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Warszawa 2020, art. 72.

[14] GIIF, *Komunikat nr 11 w sprawie raportowania*, https://www.gov.pl/web/finanse/komunikat-nr-11-w-sprawie-raportowania-do-giif-informacji-o-transakcjach-ponadprogowych-o-ktorych-mowa-w-art-72-ust-1-pkt-1-i-2-ustawy-aml (data dostępu: 11 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- art. 2 ust. 1 pkt 15 (doradcy podatkowi – w zakresie doradztwa podatkowego niewskazanego w art. 2 ust. 1 pkt 14 oraz biegli rewidenci),
- art. 2 ust. 1 pkt 18 (pośrednicy w obrocie nieruchomościami)[15].

Zgodnie z art. 105 ustawy o przeciwdziałaniu osoby uprawnione do uzyskani informacji od Generalnego Inspektora muszą złożyć pisemny wniosek. Mowa jest o organach uprawnionych i informacji, które są w posiadaniu GIFF. Ustawodawca wskazał organy podległe ministrowi spraw wewnętrznych i administracji, które to mogą złożyć pisemny wniosek o wydanie informacji od GIFF. Organy takie jak CBA czy szef ABW muszą posiadać też zgodę Prokuratora Generalnego. GIFF na wniosek przekaże również informacje zebrane Szefowi Krajowej Administracji Skarbowej oraz podległych mu służb w zakresie ich ustawowych zadań[16]. Ustęp 6 artykułu wskazuje również, jakie są przypadki, kiedy to GIFF może odmówić wydania posiadanych informacji. Takie przypadki są dwa. Jeśli GIFF uzna, że wydanie informacji może oddziałać negatywnie na trwające w GIIF procesy odmówi wydania informacji. Zachowa się tak również, gdy uzna, że wydanie tej informacji może narazić osobę bądź podmiot na niewspółmierną szkodę.

W paragrafie 106 ustawy o przeciwdziałaniu praniu brudnych pieniędzy i finansowaniu terroryzmu ustawodawca wskazał, że również Komisja Nadzoru Finansowego ma prawo uzyskania informacji od GIFF, jeśli posiada informacje o podejrzeniu prania pieniędzy lub finansowania terroryzmu[17].

Generalny Inspektor przedstawia Prezesowi Rady Ministrów roczne sprawozdanie ze swojej działalności w ciągu 3 miesięcy od zakończenia roku sprawozdawczego. Takie roczne sprawozdanie publikowane jest również na oficjalnej stronie rządowej gov.pl. Sprawozdanie zawiera w szczególności liczbę zgłoszonych przez instytucje obowiązane transakcji. Z raportu za 2020 r. wynika, iż w roku tym zarejestrowano w GIFF 3805 transakcji podejrzanych tzw. SAR-ów, które to zostały włączone do postępowań analitycznych. Dla zobrazowania, jak rośnie skala przestępstw, dodać należy, że w 2001 r. tych zgłoszeń było 231 a w 2019 r. aż 4100[18].

W 2020 r. GIIF otrzymał informacje o 33,37 mln tzw. transakcji ponadprogowych (w których równowartość przekracza ustawowy próg) oraz 894 tys. informacji korygujących. Minister sprawiedliwości przekazuje również GIIF informacje o liczbie postępowań karnych w przestępstwach, o których mowa w art. 165a kk,

[15] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2021 r., poz. 1132 z późn. zm.).

[16] E. Patsiotos (w:) *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Warszawa 2020, art. 105.

[17] E. Patsiotos (w:) *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Warszawa 2020, art. 106.

[18] Sprawozdanie GIIF za 2020 r., file:///C:/Users/admin/Downloads/Sprawozdanie_GIIF_za_2020_r_%20(1).pdf (data dostępu: 19 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

oraz wartościach majątkowych, jakie zostały zamrożone, zablokowane czy wstrzymane. GIFF podlega kontroli NIK.

Najwyższa Izba Kontroli w wydanej informacji w 2011 r. z przeprowadzonej kontroli GIFF uznała, że Generalny Inspektor Informacji Finansowej, poza nielicznymi przypadkami uchybień i nieprawidłowości, realizował zadania określone w ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[19]. NIK zwrócił uwagę, iż GIFF opóźnia procesy wydawania pozwoleń rejestracyjnych, jak również zmniejszyła się liczba przeprowadzonych kontroli w jednostkach obowiązanych. Przyczyną tych mniejszych kontroli miało być nałożenie na siedmioosobowy wydział kontroli DIF obowiązku realizowania zadań niekontrolnych. Wskazał NIK również na problemy dotyczące braku oprzyrządowania informatycznego czy braku skuteczności w wyjaśnianiu transakcji ponadprogowych.

GIIF wszczyna i prowadzi postępowania analityczne podejrzanych transakcji, które mogą mieć związek z praniem brudnych pieniędzy czy finansowaniem terroryzmu. Postępowanie wszczyna na podstawie złożonych mu zawiadomień. GIIF również może nakładać kary administracyjne. Wszystkie kontrole przeprowadzone są pisemnie przez uprawnionych pracowników posiadających upoważnienie do kontroli wydane przez Generalnego Inspektora. W czasach covid takie pisemne zawiadomienie o wszczęciu postępowania kontrolnego można przesłać za pomocą środków komunikacji internetowej. Generalny Inspektor nakłada karę pieniężną w formie decyzji, zaś kara ta stanowi dochód budżetu państwa, nie trafia ona do finansów samorządów.

10.2.2. JEDNOSTKI WSPÓŁPRACUJĄCE (ORGANY PODATKOWE I CELNE)

Jednostka informacji finansowej współpracuje również z innymi jednostkami współpracującymi, jakimi są organy kontroli skarbowej, organy podatkowe i celne. W myśl art. 8 ustawy o kontroli skarbowej organami kontroli skarbowej są:

- minister właściwy do spraw finansów publicznych jako naczelny organ kontroli skarbowej,
- Generalny Inspektor Kontroli Skarbowej jako organ wyższego stopnia nad dyrektorami urzędów kontroli skarbowej,
- dyrektor urzędu kontroli skarbowej[20].

[19] NIK, *Informacja o wynikach kontroli*, https://www.nik.gov.pl/plik/id,3369,vp,4270.pdf (data dostępu: 19 września 2021).

[20] Ustawa z dnia 28 września 1991 r. Kontrola skarbowa (t.j. Dz.U. z 2016 r., poz. 720 z późn. zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Zgodnie z art. 13 ustawy ordynacja podatkowa organami podatkowymi m.in. są:

- naczelnik urzędu skarbowego, naczelnik urzędu celno-skarbowego, wójt, burmistrz (prezydent miasta), starosta albo marszałek województwa jako organ pierwszej instancji,
- naczelnik urzędu skarbowego jako organ odwoławczy w zakresie decyzji, o których mowa w art. 83 ust. 4 i 5 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej,
- dyrektor izby administracji skarbowej – jako organ odwoławczy od decyzji naczelnika urzędu skarbowego albo naczelnika urzędu celno-skarbowego, jako organ pierwszej instancji na podstawie odrębnych przepisów, jako organ odwoławczy od decyzji wydanej przez ten organ w pierwszej instancji,
- samorządowe kolegium odwoławcze jako organ odwoławczy od decyzji wójta, burmistrza (prezydenta miasta), starosty albo marszałka województwa[21].

W postępowaniu celnym zaś organami właściwymi są naczelnik urzędu celno-skarbowego jako organ pierwszej instancji, dyrektor izby administracji skarbowej szef KAS, czyli Krajowej Administracji Skarbowej, minister właściwy do spraw finansów publicznych[22].

Organy wymienione powyżej mają obowiązek zawiadomienia Generalnego Inspektora o każdej transakcji, czynności, która może mieć związek z przestępstwem penalizowanym w art. 165a kodeksu karnego. Przepis ten stanowi o karze za finansowanie przestępstw o charakterze terrorystycznym. Organy celne mają obowiązek raportowania informacji, o których mowa w art. 5 rozporządzenia (WE) nr 1889/2005 Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie kontroli środków pieniężnych wwożonych do Wspólnoty lub wywożonych ze Wspólnoty[23]. Ponadto GIIF może zażądać od organów kontroli skarbowej czy też organów podatkowych zbadania legalności pochodzenia określonych wartości majątkowych. W 2011 r. według raportu GIFF takich wniosków zostało złożonych 13. Wniosek zawierał prośbę o zbadanie legalności tych wartości, czy nie pochodzą z podejrzanych transakcji. Taka zwrotna informacja z organów podatkowych musi zostać przekazana bezzwłocznie[24].

GIIF dokonał w 2020 r. ponad 673 blokad rachunków bankowych, na których zgromadzono ponad 246,2 mln zł. Przekazał do uprawnionych organów i jednostek 498 informacji z własnej inicjatywy. Najwięcej powiadomień z własnej inicjatywy GIIF w 2020 r. przesłał do Krajowej Administracji Skarbowej (160) i na Policję (130). Zgłoszenia, które przyjmuje GIFF, zostają przekazywane do urzędów skarbo-

[21] Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (t.j. Dz.U. z 2021 r., poz. 1540 z późn. zm.).

[22] Ustawa z dnia 19 marca 2004 r. Prawo celne (t.j. Dz.U. z 2020 r., poz. 1382 z późn. zm.).

[23] Dz.U. nr 141, poz. 1178 ze zm.

[24] *Sprawozdanie GIFF za 2020 r.*, file:///C:/Users/admin/Downloads/Sprawozdanie_GIIF_za_2020_r_.pdf (data dostępu: 19 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wych, izb administracji skarbowych, policję czy prokuraturę. Wszystkie zgłoszenia dotyczyły realnych możliwości naruszeń w obszarze naruszeń przepisów przeciwdziałania praniu brudnych pieniędzy czy finansowaniu terroryzmu. GIFF w 2020 r. otrzymał 190 wniosków od naczelników urzędów celno-skarbowych o sprawdzenie 714 podmiotów. Widoczny jest więc spadek tych wniosków w porównaniu do 2019 r., gdzie wpłynęło wnioski dla 1473 podmiotów. Pomimo faktu że wniosków tych jest mniej, ewidentnie można zauważyć zwiększenie skuteczności współpracy GIIF z KAS. Współpraca ta ma na celu odcinać przestępców od środków finansowych pozyskanych nielegalnie i próbujących dokonać transakcji prania pieniędzy. Dyrektorzy Izb Administracji Skarbowej wystosowali w 2020 r. aż 127 wniosków o sprawdzenie 806 podmiotów pod kątem legalności przeprowadzonych transakcji. Również KAS otrzymuje informacje od GIIF w zakresie swoich ustawowych zadań. Uzyskane informacje KAS wykorzystuje do analiz i czynności sprawdzających podatników. Pozyskane informacje często stanowią podstawę do wszczęcia postępowania kontrolnego podatnika. Celem tych działań jest prawidłowa egzekucja podatków i zabezpieczenie należności Skarbu Państwa. Należy tu zaznaczyć, że to właśnie KAS jest tym organem, który ma za zadanie realizację dochodów z budżetu państwa.

10.2.3. AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO I AGENCJA WYWIADU

Szefowie agencji ABW i AW wykonują czynności związane z przeciwdziałaniem finansowaniu terroryzmu. Agencje te również pełnią ważną rolę w przeciwdziałaniu praniu brudnych pieniędzy i finansowaniu terroryzmu. Są jednostkami współpracującymi z GIIF podobnie jak wszelkiego rodzaju organy podatkowe.

ABW ma za zadanie głównie rozpoznawać formy prania pieniędzy. Na oficjalnej stronie ABW można znaleźć opis przykładowych metod prania pieniędzy. Są to np.

- smurfing; polega na wpłacaniu przez podstawionych ludzi niewielkich kwot, co nie wymaga kontroli tożsamości podmiotów biorących udział w transakcji,
- mieszanie; polega na wymieszaniu pieniędzy pochodzących z przestępstw pod legalnie prowadzony biznes,
- puste transakcje; polega na wprowadzeniu w obrót tzw. pustych faktur i transakcji nie mających nigdy miejsca. Transakcje te są typowe dla karuzeli podatkowych w VAT. Puste faktury mogą jednak stanowić idealną sytuację dla wyprowadzenia środków finansowych.

Bardzo często to właśnie ABW rozpracowuje „pralnie pieniędzy". W czerwcu 2021 r. agenci ABW rozpracowali w Warszawie i Radomiu pralnię brudnych pieniędzy, wskutek czego zatrzymano 3 osoby. Osoby te wyprały ponad miliard

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

złotych, a środki pieniężne, które zasilały rachunki bankowe fikcyjnych spółek, pochodziły głównie z Rosji. W proceder zamieszany był mężczyzna i dwie kobiety pracujące w banku, które otwierały rachunki bankowe dla fikcyjnych spółek otwieranych na prezesach słupach. Prezes słup to osoba pozyskana z zewnątrz, opłacona, nie mająca pojęcia o tym, co robi firma, w której jest najważniejszą osobą[25].

Służba ta jest uprawniona do dokonywania czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych w celu rozpoznania, wykrywania i zapobiegania przestępstwom. Nowa ustawa nie uprawniła polskiej jednostki analityki finansowej PJAF o takie instrumenty śledcze, dlatego też GIFF musi współpracować z takimi podmiotami, które zostały wyposażone w takie kompetencje. Jednym z obowiązków jednostek współpracujących, o czym już wspomniano, jest przekazywanie na wniosek informacji do GIIF. Dotyczy to również ABW, która na podstawie art. 82 nuop je sporządza i przekazuje do GIFF. ABW jest jedną z nielicznych jednostek współpracujących mających status służby specjalnej. Służba ta przejawia się w trosce o bezpieczeństwo kraju. ABW dokonuje szybkiej reakcji, jeśli uzyska wiedzę na temat podejrzenia popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, jeśli dokona porównania podejrzenia z raportem uzyskanym od GIFF. Dlatego ważnym elementem jest niezwłoczność działania, GIFF ma aż 30 dni na odpowiedź zwrotną i wydaje się, że jest to dość długi okres, zwłaszcza w sytuacji potencjalnego zagrożenia terrorystycznego, gdzie ważny jest każdy dzień, gdzie należałoby na przykład dokonać zabezpieczenia w postaci blokady rachunku bankowego. W ramach prowadzonych czynności analitycznych GIFF pozyskuje informacje w różny sposób, jeśli GIIF złożył zawiadomienie o podejrzeniu popełnienia przestępstwa na postawie informacji pozyskanej od instytucji współpracującej, w tym ABW, informuje ją zwrotnie w terminie nie późniejszym niż 30 dni.

GIFF przekazuje do prokuratury informację o podejrzeniu popełnienia przestępstwa, jednak jego rola się na tym nie kończy. Jeśli Prokuratura zażąda od Generalnego Inspektora dokumentacji czy informacji, ich udostępnienia, to, jeśli sam nie dysponuje nimi, kieruje wniosek do jednostek współpracujących, w tym do ABW[26].

Szef Agencji Bezpieczeństwa Wewnętrznego oraz Szef Agencji Wywiadu są centralnymi organami administracji rządowej działając za pomocą agencji będącymi agencjami administracji rządowej[27].

[25] ABW, https://www.abw.gov.pl/pl/informacje/1848,ABW-rozbila-quotpralniequot-pieniedzy.html (data dostępu: 19 września 2021).

[26] M.A. Kędzierski., *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Przegląd Bezpieczeństwa Narodowego" 2020, nr 22 (12).

[27] P. Przybysz, *3. Naczelne i centralne organy administracji rządowej* (w:) *Instytucje prawa administracyjnego*, Wolters Kluwer, Warszawa 2020.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

10.3. ORGANY PODATKOWE W WALCE Z PRZESTĘPCZOŚCIĄ PRANIA PIENIĘDZY

Przepis karny w art. 299§1 k.k. w sposób podstawowy wyraża, czym jest pranie pieniędzy w świetle przepisów karnych. Zgodnie z tym artykułem:

„Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku”[28].

Odpowiedzialność karna za pranie pieniędzy wymaga udowodnienia winy od sprawcy czynu zabronionego, gdyż w prawie karnym zasadą jest, że czyn musi być zabroniony i społecznie szkodliwy, a sprawcy można przypisać karę. W przypadku prania pieniędzy trudno stwierdzić, że czyn ten nie jest społecznie szkodliwy[29]. Dodatkowo pranie pieniędzy z art. 299§1 k.k. uderza w „dobra prawnie chronione w ramach kryminalizacji jego czynów bazowych”[30].

Przestępczość podatkowa jest tak samo szkodliwa jak inne czyny zabronione, przede wszystkim szkodliwie wpływa na dochody budżetu państwa, a tym samym negatywnie oddziałuje na każdego obywatela. Największa przestępczość związana jest z oszustwami w systemie VAT głównie poprzez karuzele VAT, które powodują tworzenie tzw. luki w VAT. Luka w podatku VAT jest o tyle ważna, że niszczy gospodarkę. Organy podatkowe szacują zawsze wysokość podatku, jaka powinna wpłynąć do budżetu, ta część, która nie wpłynie, jest luką w VAT. W latach 2008–2015 wynosiła ona 250 mld zł[31].

Kodeks karno-skarbowy w dziale II części szczególnej wymienia, czym są przestępstwa o podłożu karno-skarbowym, są to m.in. nieujawnienie przedmiotu lub podstawy opodatkowania, firmactwo, oszustwa podatkowe, uporczywe niepłacenie podatków, dokonywanie płatności z pominięciem mechanizmu podzielonej płatności, brak księgi, uchybienia w prowadzeniu ksiąg, paserstwo akcyzowe,

[28] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2020 r., poz. 1444 ze zm.).

[29] *System prawa karnego*, t. 9, *Przestępstwa przeciwko mieniu i gospodarcze*, red. R. Zawłocki, Warszawa 2015, s. 586.

[30] *Kodeks karny*, t. III, *Komentarz do art. 278–363 k.k., Komentarz do art. 299 k.k., pkt. 7*, red. A. Zoll.

[31] *Luka w VAT*, https://demagog.org.pl/wypowiedzi/luka-vat-w-polsce-sprawdzamy-dane-nik/ (data dostępu: 21 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

bezprawność czynności handlowej[32]. W znaczącym też stopniu można połączyć k.k.s z przepisami k.k., czyli dojść do zbiegu kumulatywnego. Taka sytuacja może się zdarzyć, gdy podatnik wystawi tzw. pustą fakturę, czyli bez podstawy jej wystawienia, art. 77 k.k.s stanowi, że fałszywym dokumentem jest również pusta faktura, gdyż w sposób fałszywy obrazuje rzeczywistość. Jeśli na tej podstawie podatnik uzyska nadpłatę podatku VAT, może dostać również zarzut z art. 228 k.k. Pusta faktura może również posłużyć do zapłaty, czyli do wprowadzenia do obrotu „brudnych" pieniędzy.

Konstrukcja prawa karnego i odpowiedzialności karnej za pranie pieniędzy wymaga, aby korzyści związane były z popełnionym czynem zabronionym. Z przyjętej doktryny można stwierdzić, że chodzi o związek z jakimkolwiek czynem zabronionym. Dotyczy to wszystkich przestępstw określonych w kodeksie karnym oraz w innych ustawach, które to czyny noszą znamiona przestępstw lub przestępstw skarbowych[33].

Można spotkać w komentarzach zapis, że ukrywanie legalnego majątku przed organami podatkowymi nie stanowi prania pieniędzy i nie znajduje się w przepisie art. 299 k.k., gdyż nie pochodzi z czynów nielegalnych, lecz jest wynikiem pracy w działalności gospodarczej. Niemniej są osoby, które tego poglądu nie popierają. Art. 54 k.k.s stanowi, że „podatnik, który uchylając się od opodatkowania, nie ujawnia właściwemu organowi przedmiotu lub podstawy opodatkowania lub nie składa deklaracji, przez co naraża podatek na uszczuplenie, podlega karze"[34]. Z tak sformułowanego przepisu wynika, że każde uszczuplenie może być przedmiotem odpowiedzialności karnej na podstawie k.k.s., a tym samym stać się przedmiotem prania pieniędzy. Taka też interpretacja przepisów przeważa w literaturze[35].

Trudno jest się więc dziwić, że państwo i ich administracja podatkowa wymyśla coraz to nowe narzędzia i sposoby radzenia sobie z tego rodzaju przestępstwami.

10.3.1. KRAJOWA ADMINISTRACJA SKARBOWA

Krajowa Administracja Skarbowa została powołana w dniu 1 marca 2017 r. ustawą o Krajowej Administracji Skarbowej. Krajowa Administracja Skarbowa podlega ministrowi ds. finansów publicznych. Zastąpiła niejako administrację podatkową,

[32] Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (t.j. Dz.U. z 2021 r., poz. 408 ze zm.).

[33] A. Marek, *Kodeks karny.* Komentarz do art. 299 kodeksu karnego, LEX, 2010, pkt 2.

[34] Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (t.j. Dz.U. z 2021 r., poz. 408 ze zm.).

[35] K. Buk, „*Pranie brudnych pieniędzy*" *pochodzących z korzyści związanych z popełnieniem czynów zabronionych skierowanych przeciwko obowiązkom podatkowym*, „Doradca Podatkowy" 2006, nr 5, s. 54,

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

kontrolę skarbową oraz służbę celną. Organy te zostały zniesione i powołano do życia nowe. KAS to obecnie kontrola i podatkowa, i celna, i posiada ogromną ilość uprawnień. Ustawa zniosła stanowisko Generalnego Inspektora Kontroli Skarbowej, Szefa Służby Celnej, dyrektorów izb skarbowych, dyrektorów urzędów kontroli skarbowej oraz naczelników urzędów skarbowych. Powołano natomiast Szefa Krajowej Administracji Skarbowej, dyrektora Krajowej Informacji Skarbowej, dyrektora izby administracji skarbowej oraz naczelnika urzędu celno-skarbowego[36].

Ustawa o Krajowej Administracji Skarbowej wprowadziła dotąd nieznany rodzaj kontroli, tj. kontrolę karno-skarbową. Krajowa Administracja Skarbowa, dalej KAS, może wszcząć kontrolę w celu sprawdzenia podatnika, czy przestrzega przepisy prawa podatkowego. Podmiotem kontroli mogą być osoby fizyczne, prawne lub jednostki niemające osobowości prawnej, lecz zobowiązane są do przestrzegania prawa podatkowego. Podstawową grupą kontrolowaną są przedsiębiorcy, lecz często dochodzi do kontrolowania podmiotów, które z uwagi na to, czym się zajmują, są obiektem kontroli. Mowa tutaj przykładowo o osobach prywatnych, importerach towarów nabytych na zagranicznych portalach aukcyjnych. Kontrola z KAS może dotyczyć prawa podatkowego, celnego, gier hazardowych, prawa dewizowego, prania pieniędzy i finansowania terroryzmu. Co ważne, do kontroli celno-skarbowej nie stosuje się przepisów z rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo Przedsiębiorców. Oznacza to, że KASA może przeprowadzić kontrolę celno-podatkową bez zawiadomienia o zamiarze jej wszczęcia, nie musi posiadać upoważnienia do przeprowadzenia kontroli, obecność kontrolowanego nie jest wymagana, nie stosuje się w stosunku do tej kontroli z góry określonych limitów czasu na przeprowadzenie kontroli[37].

Głównym zadaniem Krajowej Administracji Skarbowej jest realizacja dochodów z podatków, należności celnych, podatkowych i niepodatkowych należności budżetowych. Powinien zapewnić obsługę i wsparcie podatnika i przedsiębiorcy w prawidłowym wykonywaniu obowiązków podatkowych i celnych. Ustawa nakłada też inne obowiązki, które są katalogiem otwartym, m.in. KAS ma obowiązek wykrywania i ścigania sprawców niektórych przestępstw wymienionych w ustawie. W art. 2§1 pkt. 15 ustawodawca wprost wymienił art. 299 kk jako obowiązek KAS do ścigania przestępstw prania pieniędzy i finansowania terroryzmu[38]. Tak więc od 1 marca 2017 r. do zadań KAS należy przeciwdziałanie

[36] M. Łoboda, D. Strzelec, *1.3. Zadania Krajowej Administracji Skarbowej* (w:) *Kontrola przestrzegania przepisów prawa podatkowego*, M. Łoboda, D. Strzelec, Wolters Kluwer, Warszawa 2017.

[37] A. Kraszewski, K. Krzal (w:) *Prawo przedsiębiorców. Komentarz*, red. A. Pietrzak, Wolters Kluwer, Warszawa 2019, art. 62.

[38] M. Łoboda, D. Strzelec, *1.3.4. Zadania w zakresie zwalczania przestępczości* (w:) *Kontrola przestrzegania przepisów prawa podatkowego*, M. Łoboda, D. Strzelec, Wolters Kluwer, Warszawa 2017.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

praniu pieniędzy, do końca lutego 2017 r. zadania te wykonywał minister właściwy do spraw instytucji finansowych oraz Generalny Inspektor Informacji Finansowej.

Dodać należy również, że KAS uzyskała nowe uprawienia do walki z karuzelami podatkowymi. Organ ten jest zobligowany do wykrywania, zapobiegania i zwalczania przestępstw wymienionych w art. 2 ust. 1 pkt. 15 u.k.a.s., a dotyczący przestępczości zorganizowanej czy udziału w zorganizowanej grupie przestępczej[39].

10.3.2. CZYNNOŚCI OPERACYJNO-ROZPOZNAWCZE ORGANÓW KRAJOWEJ ADMINISTRACJI SKARBOWEJ

Krajowa Administracja Skarbowa otrzymała wiele szczegółowych uprawnień, które wydawać by się mogło ograniczają prawa i wolności obywatelskie. W uzasadnieniu do ustawy o KAS wskazano jednak, że regulacje te nie mają prowadzić do zwiększenia represyjności aparatu skarbowego. Ustawodawca podkreśla również, że czynności operacyjno-rozpoznawcze należy uznać, w świetle norm konstytucyjnych[40], metody muszą zostać użyte proporcjonalnie do zwalczania przestępczości skarbowej, w szczególności w zakresie podatku VAT. Ich stosowanie ma być nierozłączne z uznaniem, że są konieczne w demokratycznym państwie dla jego bezpieczeństwa i dobra kraju.

Czynności operacyjno-rozpoznawcze, jakimi może posłużyć się Krajowa Administracja Skarbowa, to:

- prowadzenie obserwacji zgodnie z art. 17 ustawy o KAS,
- stosowanie kontroli zgodnie z art. 18 ustawy o KAS,
- pozyskanie danych telekomunikacyjnych i ich udostępniania zgodnie z art. 114–115 ustawy o KAS,
- niejawne nadzorowanie wytwarzania, przemieszczania i przechowywania przedmiotów przestępstwa oraz obrotu nimi zgodnie z art. 120 ustawy o KAS,
- zakup kontrolowany (nowe rozwiązanie) lub też możliwość wręczenia korzyści majątkowych.

Stosowanie kontroli polega na możliwości uzyskiwania i zapisu rozmów telefonicznych, utrwalania obrazu lub dźwięku, przechwytywania korespondencji w tym tej elektronicznej.

Uwzględniono również możliwość gromadzenia danych na temat podmiotu będącego celem kontroli skarbowej, jeśli zachodzi podejrzenie popełnienia prze-

[39] *Ibidem*.

[40] Konstytucja Rzeczypospolitej Polski z dnia 2 kwietnia 1997 r. (t.j. Dz.U. nr 78, poz. 483 ze zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

stępstwa albo przestępstwa skarbowego. Taka możliwość zawarta jest w art. 113 ustawy KAS. Dodatkowo w ramach art. 113 ustawy o KAS organ ten otrzymał szczególne uprawnienia do zatrzymania i przeszukania osób, zatrzymania rzeczy, przeszukania lokalu mieszkalnego, pomieszczeń, bagażników, garaży, generalnie każdego miejsca, jeśli są uzasadnione potrzeby konieczności przeszukania. KAS może również zatrzymać w pościgu osobę, o której mowa w art. 20 Konwencji sporządzonej na podstawie art. K3 Traktatu Unii Europejskiej w sprawie wzajemnej pomocy i współpracy między administracjami celnymi[41]. KASA może również brać udział w konwoju, o którym mowa w ustawie o środkach masowego przymusu i broni palnej[42]. Ponadto funkcjonariusze mogą używać broni palnej w celu realizacji zadań[43].

10.4. BLOKADA RACHUNKU BANKOWEGO PODMIOTU KWALIFIKOWANEGO

STIR jest zbudowanym systemem teleinformacyjnym izby rozliczeniowej i ma generalnie 3 zadania. Głównym jego celem jest odbieranie i przetwarzanie danych w celu ustalenia ryzyka. Wskaźnikiem ryzyka jest wskaźnik wykorzystywania działalności banków i spółdzielczych kas oszczędnościowo-kredytowych do wyłudzeń skarbowych. Kolejnym zadaniem jest przekazanie tej informacji do Centralnego Rejestru Danych Podatkowych, dalej CRDP, oraz systemów teleinformacyjnych banków i spółdzielczych kas oszczędnościowo-kredytowych. Ponadto STIR służy do przesyłania danych między szefem KAS a bankami i Skokami, w tym związanych z blokadami rachunków bankowych[44].

Przepisy umożliwiające szefowi KAS blokadę rachunku bankowego podmiotu kwalifikowanego obowiązują od 30 kwietnia 2018 r., pewne modyfikacje zostały wprowadzone w sierpniu 2018 r. i lipcu 2019 r.

Narzędzie to może być skuteczną formą walki z przestępczością podatkową zwłaszcza na poziomie wyłudzeń VAT. Głównie chodzi o tzw. znikającego podatnika. W karuzeli podatkowej bierze udział kilka podmiotów, który każdy pełni

[41] Dz.U. z 2008 r., nr 6, poz. 31.

[42] Obwieszenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 11 maja 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy o środkach masowego przymusu i broni palnej (t.j. Dz.U. z 2017 r., poz. 1120).

[43] A. Podsiadły, J. Zawiejska-Rataj, *Rozpoznawanie, wykrywanie, ściganie i zwalczanie czynów zabronionych, zapobieganie im i ściganie ich sprawców przez organy Krajowej Administracji Skarbowej*, „Przegląd Podatkowy" 2017, nr 10, s. 37.

[44] M. Niezgódka-Medek (w:) *Ordynacja podatkowa. Komentarz*, art. 119(zha)*, wyd. XI*, S. Babiarz, B. Dauter, R. Hauser, A. Kabat, J. Rudowski, M. Niezgódka-Medek, Wolters Kluwer, Warszawa 2019.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

inną funkcję w procederze karuzeli podatkowej. Znikający podatnik rejestruje firmę i rejestruje się jako podatnik VAT czynny. Wystawia faktury, oczywiście, najczęściej tzw. puste przedstawiające fikcyjne transakcje i znika nie płacąc VAT lub prosi organ podatkowy o zwrot podatku VAT z tytułu jego nadpłaty. Jeśli podmiot taki wystawia faktury na stawkę VAT 0 procent, to powstanie u niego nadpłata z tytułu VAT naliczonego, po otrzymaniu wyłudzonego podatku podmiot taki znika[45].

Blokada rachunku powoduje możliwość zabezpieczenia środków pieniężnych przed wyprowadzeniem ich z rachunku bankowego. Wspomniany znikający podatnik wystawił faktury sprzedaży z VAT na ogromne sumy, powinien zapłacić VAT do izby skarbowej, ale tego nigdy nie zrobi i zniknie. Dlatego też Szef KAS ma możliwość zareagowania w odpowiedni sposób i zamiast zablokować pojedyncze transakcje, może unieruchomić środki pieniężne zgromadzone na rachunku bankowym nawet do 72h. W uzasadnionych przypadkach termin ten może zostać wydłużony do trzech miesięcy[46].

Blokada środków zgromadzonych na rachunku powinna być stosowana ostrożnie i nigdy nie powinna zostać zastosowana w stosunku do podmiotów/podatników uczciwych. Z przepisów art. 119 o.p. wyczytać też można, że blokada może zostać również dokonana na rachunku, którego podmiot kwalifikowany jest współposiadaczem. Blokowane są środki w każdej walucie, a od blokady można złożyć zaskarżenie. Mimo że jest to skuteczna forma walki z przestępczością podatkową czy praniem pieniędzy, ingeruje się jednak w sposób istotny w konstytucyjne prawo własności[47].

Szef KAS może wyrazić zgodę na częściowe zwolnienie blokady na przykład na możliwość wypłaty wynagrodzeń lub uchylić blokadę, jeśli jego zdaniem okoliczności blokady ustąpią[48].

10.5. JEDNOLITY PLIK KONTROLNY

Jednolity plik kontrolny to kolejne potężne narzędzie z przestępczością podatkową. Głównym jego celem było ograniczenie możliwości wyłudzeń VAT.

---

[45] I. Ożóg, *Karuzele i inne oszustwa podatkowe. Metody przeciwdziałania unikaniu opodatkowania*, Wolters Kluwer, Warszawa 2021.

[46] K. Teszner, *Ordynacja podatkowa. Komentarz aktualizowany*, Wolters Kluwer, Warszawa 2021, art. 119(zv).

[47] S. Babiarz, B. Dauter, R. Hauser, A. Kabat, M. Niezgódka-Medek, J. Rudowski, *Ordynacja podatkowa. Komentarz,* Wolters Kluwer, Warszawa 2019, s. 684.

[48] B. Brzeziński, K. Lasiński-Sulecki, W. Morawski, *2.2.2. Blokada rachunku bankowego* (w:) Nowe *narzędzia kontrolne, dokumentacyjne i informatyczne w prawie podatkowym*, B. Brzeziński i in., Wolters Kluwer, Warszawa 2018.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Od 1 stycznia 2018 r. jest obowiązkowy dla wszystkich podatników będących podatnikami czynnymi w VAT. JPK został wprowadzony pierwotnie już w 2015 r., lecz początkowo nie obejmował swoim zasięgiem wszystkich podatników. JPK obecnie to JPK-VAT i jest deklaracją podatku VAT oraz ewidencją zakupów i sprzedaży. Składa się ją elektronicznie w formie dokumentu XML do urzędów skarbowych w terminie wynikającym z ustawy podatkowej. JPK ma część deklaracyjną i ewidencyjną. W części ewidencyjnej podatnicy wykazują wszystkie faktury zakupu i sprzedaży. Organ podatkowy otrzymuje więc ogromną ilość informacji na temat, gdzie podatnik dokonuje zakupów towarów czy usług, jak również w pigułce otrzymuje dane kontrahentów jego sprzedaży[49]. Taki sposób raportowania daje organom podatkowym możliwość weryfikacji bez przeprowadzania kontroli poprawności złożonego raportu. Przy JPK-VAT nie ma możliwości, aby faktura pusta, która została wykazana tylko z jednej strony transakcji, nie została przechwycona przez organy podatkowe. Warto też dodać, że organy podatkowe mają wgląd bezpośrednio na rachunki bankowe podatnika prowadzącego działalność gospodarczą. Mają więc wszystkie narzędzia, aby zweryfikować, czy faktura została wystawiona prawidłowo, czy druga strona dokonała zapisu w swoich księgach i czy została opłacona rachunkiem bankowym. Na rządowej stronie można również uzyskać informację, że wprowadzenie tego mechanizmu ma na celu zmniejszenie ilości przeprowadzanych kontroli u podatnika oraz automatyczną weryfikację kwot wykazanych na deklaracji[50].

10.6. MECHANIZM PODZIELNEJ PŁATNOŚCI

Mechanizm podzielnej płatności, czyli MPP, zwany split payment, to kolejny cios w nieuczciwych podatników i potencjalnych przestępców skarbowych. Polega on na płatności podzielonej dla transakcji powyżej 15 000,00 zł i przymus taki jest obligatoryjny dla transakcji kupna towarów i usług z załącznika 15 ustawy o VAT. W załączniku tym wykazane są tzw. towary wrażliwe, gdzie przy handlu tymi towarami najwięcej było wyłudzeń na płaszczyźnie podatku od towarów i usług. Wśród nich znajdują się paliwa, wyroby ze stali, elektronika, części samochodowe, niektóre usługi budowlane. Płatności są obligatoryjne tylko dla pojedynczych transakcji zafakturowanych powyżej 15 000,00 zł i na fakturze powinien zostać dopisany skrót MPP.

Taka informacja dla płacącego za fakturę jest istotna, bowiem dowiaduje się wówczas, że musi dokonać płatności podzielonej. Split payment polega na

[49] A. Bartosiewicz, M. Smaga*, E-kontrola podatkowa i jednolity plik kontrolny*, Wolters Kluwer, Warszawa 2018, s. 1.

[50] Jednolity Plik Kontrolny, https://www.podatki.gov.pl/jednolity-plik-kontrolny/jpk-vat-z-deklaracja/jpk-vat-z-deklaracja-info (data dostępu: 21 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

zapłacie za fakturę w sposób podzielony, przy jednym przelewie wskazuje kwotę netto i VAT z faktury zakupu i dopisuje NIP podmiotu, od którego dokonywało się zakupów. Bank kieruje wówczas kwotę VAT nie na konto bieżące podmiotu, lecz na konto techniczne podatku VAT. Konto VAT nie jest rachunkiem, z którego podatnik może korzystać w dowolny sposób. Nie może dokonywać z niego innych płatności jak tylko płatności o charakterze danin publicznych. Może z tego konta uregulować swój podatek VAT czy podatek dochodowy lub ZUS, ale już innej zlecić z tego konta nie może.

Istotne jest to, że w przypadku, kiedy podatnik dokonuje zwrotu podatku VAT w związku z nadpłatą tego podatku i przekieruje zwrot na swój techniczny rachunek VAT w banku otrzyma go bez czynności sprawdzających w terminie do 25 dni[51].

Oczywiście, zdarzają się przypadki, gdzie kupujący pomyli się we wprowadzaniu danych i zamiast wysłać netto na konto dostawcy prześle VAT, zaś VAT na konto bieżące. Nie ma jednak żadnej możliwości wycofania takiej dyspozycji czy poproszenia banku o zmianę transakcji. Zebrane środki na koncie VAT mogą zostać przekazane na rachunek bieżący tylko za zgodą naczelnika urzędu skarbowego po rozpoznaniu pozytywnym wniosku o takie przeniesienie środków[52].

10.7. PODSUMOWANIE

Proceder prania brudnych pieniędzy był wiele razy przedmiotem badań naukowych. Jego skala i wielopłaszczyznowość są zjawiskiem ogromnym i bardzo niebezpiecznym dla gospodarek państw i ich budżetów. Walka z tego rodzajem przestępstwem jest wymagana i dotyczy nie tylko Polski czy Unii Europejskiej, ale też krajów tzw. Trzeciego Świata.

W budowie polskiego systemu walki z przestępczością prania pieniędzy ważnym aspektem było dostosowanie go do standardów europejskich. Już w 2002 r. doszło do nowelizacji ustawy Prawa Bankowego przez określenie terminu prania pieniędzy na podstawie ustawy z dnia 12 października 1994 r. o ochronie obrotu gospodarczego i zmianie niektórych przepisów prawa karnego. W 2000 r. wprowadzono ustawę o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Ważnym krokiem było powołanie do życia Generalnego Inspektora Informacji Finansowej, jak również znowelizowanie art. 299 kodeksu karnego. To wszystko sprawiło, że Polska jako kraj wdrażała europejskie standardy w swój system walki z przestępczością na tle wyłudzeń i prania brudnych pieniędzy.

[51] K. Kasprzyk, *Mechanizm podzielnej płatności,* Warszawa 2018, s. 110–111.

[52] Ł. Matusiakiewicz*, Obowiązkowy split payment*, LEX/el, Warszawa 2019, s. 23.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Człowiek jako istota ludzka zawsze będzie poszukiwać nowych dróg, by móc uzyskać korzyść finansową dla siebie, teraz w dobie zmian technicznych przestępczość zatacza coraz to nowe kręgi. Państwa całego świata walczą z przestępczością, śledzą, wyłapują i skazują za takie procedery, jednak to nie spowoduje, że przestępczość zniknie czy zaniknie w sposób zdecydowany.

Obecnie wiele instytucji musi być powiązanych, aby doszło do wykrycia próby oszustwa, organy ściśle z sobą współpracują. I współpraca taka jest konieczna w przyszłości zakładając, że będzie polepszać się sieć przekazywania sobie informacji, bardzo ważna jest niezwłoczność przekazu, ilość osób zaopatrzonych w większe kompetencje do odszukiwania takich nielegalnych transakcji. Trudno stwierdzić, że obecny system przeciwdziałania praniu brudnych pieniędzy jest wystarczający. Pracownicy instytucji obowiązanych muszą posiadać wysokie kwalifikacje, doświadczenie i bardzo specjalistyczną wiedzę, żeby móc mówić o skutecznym systemie przeciwdziałania praniu pieniędzy. Niestety, podczas analiz dochodzi często do błędów związanych właśnie z brakiem doświadczenia i wiedzy. Mało tego, często dochodzi do pomyłek w rejestracji transakcji lub podejrzane transakcje nie są wprowadzane do systemu w ogóle. Wciąż brakuje specjalistów w zakresie prawa karnego, cywilnego, bankowego, podatkowego. Zorganizowane grupy przestępcze są pod tym kątem o krok do przodu, nie oszczędzają na wyspecjalizowanej kadrze specjalistów, aby ominąć złożoną materię kontrolną. Wyszukują dróg i metod, jak obejść ten system, który jest im doskonale znany. Zawsze będzie to walka bez końca, przestępcy będą się kształcić i wymyślać, jak ominąć wprowadzane rozwiązania, które im „zawadzają". Organy państwowe natomiast będą wymyślać coraz to nowe rozwiązania, aby utrudnić ten proceder.

Należy też zauważyć jedną rzecz, która powinna budzić niepokój. Wszystkie przepisy prawa, które mają za zadanie uszczelnić system podatkowy, wpływają na zakres prawa własności. Organy podatkowe posiadają wiedzę o podatnikach i takie narzędzia do kontrolowania i blokowania ich działalności gospodarczych, że wydaje się to zbyt szerokim działaniem. Należałoby poszukać takich rozwiązań, aby podatnik nie chciał dokonywać czynów niedozwolonych, gdyż po prostu nie będzie mu się to opłacać.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Katarzyna Chudzik
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 11.

WSTRZYMANIE TRANSAKCJI I BLOKADA RACHUNKU JAKO NARZĘDZIA WALKI Z ML/FT

11.1. UWAGI WPROWADZAJĄCE

W dzisiejszych czasach, zważywszy na ogólną globalizację oraz postępujący dostęp do technologii i nowoczesnych rozwiązań, niemal każdy człowiek posiada, lub przynajmniej słyszał, o rachunku bankowym. Stanowi on ogromne ułatwienie w codziennym funkcjonowaniu oraz prowadzeniu transakcji handlowych takich jak przelewy, opłacanie rachunków czy chociażby płacenie za zakupy. Pozwala on na manipulowanie nawet dużymi kwotami pieniędzmi w krótkim czasie oraz z dowolnego miejsca na świecie lub po prostu za pośrednictwem Internetu. Rachunek bankowy jest zapisem prowadzonym przez bank w celu rejestracji wpłat i wypłat oraz innych rozliczeń, a także przechowywania środków. Zostaje ustanowiony między bankiem a posiadaczem na czas określony lub nieokreślony[1].

Jednocześnie rozwój technologii ustanowił nowe możliwość dla przestępczości finansowej. Czyny zabronione mogą być popełniane tak naprawdę w kilka kliknięć przed ekranem komputera czy telefonu. Przykładem takiej działalności jest właśnie ML/FT. Skrót ML (*money laundering*) oznacza pranie pieniędzy, czyli obrót wartościami majątkowymi pochodzącymi z popełnienia czynu zabronionego, natomiast FT (*terrorism financing*) to finansowanie terroryzmu oznaczającego dostarczanie lub gromadzenie środków przeznaczonych na działalność przestępczą. Według wyliczeń przeprowadzonych przez Ministerstwo Finansów w krajowej ocenie ryzyka prania pieniędzy oraz finansowania terroryzmu w Polsce ryzyko ogólne

[1] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2020 r., poz. 1740).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wynosi dla prana pieniędzy ok. 1,95 natomiast dla finansowania terroryzmu ok. 1,65. Zagrożenie przestępstwami bazowymi dla prania pieniędzy można oceniać na poziomie pomiędzy średnim a wysokim odnotowując jego spadek dzięki dużej wykrywalności oraz skutecznemu ograniczeniu przestępstw skarbowych. Zagrożenie finansowania terroryzmu natomiast w ostatnich latach podniosło się z poziomu niskiego na średni głównie za sprawą położenia geopolitycznego Polski oraz przez aktywność międzynarodową, które mogą zdaniem niektórych badaczy wpłynąć na atrakcyjność kraju jako miejsca rozwijania zaplecza logistycznego i finansowego przez organizacje terrorystyczne[2].

Jednym ze sposobów utrudniania popełniania lub udaremniania czynów wpisujących się w działalność ML/FT są wstrzymanie transakcji oraz blokada rachunku. Wstrzymanie transakcji zostało zdefiniowane w Ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu jako czasowe ograniczenie korzystania i dysponowania wartościami majątkowymi, polegające na uniemożliwieniu przeprowadzenia przez instytucję obowiązaną określonej transakcji lub większej liczby określonych transakcji.

Natomiast sformułowanie „blokadę rachunku" ustawodawca zdefiniował jako czasowe uniemożliwienie korzystania i dysponowania ze wszystkich lub części wartości majątkowych gromadzonych na rachunku, w tym również przez instytucję obowiązaną[3].

Celem niniejszego rozdziału jest przeanalizowanie, czy czynności te stanowią narzędzie walki państwa z ML/FT oraz jak wykorzystywane są one w prawie bankowym, a także w Ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

W rozprawie zastosowano metody badawcze zmierzające do skoordynowania sposobu postępowania z zakładanym celem badań: metoda analizy i krytyki piśmiennictwa, analiza i synteza, uogólnianie i wnioskowanie jako oparcie w procesach poznania myślowego.

[2] *Krajowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu,* https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu (data dostępu: 26 sierpnia 2021).

[3] Ustawa z dnia 1 marca 2018 r. – o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

11.2. WSTRZYMANIE TRANSAKCJI I BLOKADA RACHUNKU W USTAWIE O PRZECIWDZIAŁANIU PRANIU PIENIĘDZY ORAZ FINANSOWANIU TERRORYZMU

Jak już zostało wspomniane we wstępie, Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu jasno określa, co rozumiemy przez wstrzymanie transakcji oraz blokadę rachunku, zostało to określone w formie definicji w początkowych artykułach aktu. Ponadto w sposób enumeratywny określone zostało, co oznacza używane w ustawie hasło „rachunek". W art. 2 ust. 2 pkt. 17 wypunktowano: rachunek płatniczy, rachunek bankowy, rachunek w spółdzielczej kasie oszczędnościowo-kredytowej, rachunek papierów wartościowych, rachunek zbiorczy, rachunek pieniężny, rejestr uczestników funduszu lub ewidencję uczestników funduszu inwestycyjnego zamkniętego, prowadzony w formie elektronicznej zbiór danych identyfikacyjnych zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany, rachunek derywatów. W art. 2 ust. 2 pkt. 21 podano natomiast definicję słowa „transakcja" określając ją jako czynność prawną lub faktyczną, na podstawie której dokonuje się przeniesienia własności lub posiadania wartości majątkowych, albo czynność dokonywaną w celu przeniesienia własności lub posiadania wartości majątkowych.

Jeśli chodzi o organy administracji rządowej właściwe w sprawach przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu poza ministrem finansów istotną rolę pełni Generalny Inspektor Informacji Finansowej (zwany dalej GIIF) powoływany i odwoływany przez Prezesa Rady Ministrów na wniosek ministra właściwego do spraw finansów publicznych, po zasięgnięciu opinii ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych. GIIF jest jednym z podmiotów posiadających uprawnienia z ustawy zarówno do wstrzymania transakcji, jak i blokady rachunku[4].

W art. 12 wyżej wymienionej ustawy został określony zakres zadań GIIF. Nie jest to jednak katalog zamknięty, określa jedynie, jakie zadania, w szczególności, powinny zostać podejmowane w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Ustawodawca wyszczególnił: sprawowanie kontroli nad przestrzeganiem przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, analizę informacji o wartościach majątkowych w przypadku gdy zachodzi podejrzenie popełnienia przestępstwa, żądanie przekazania infor-

[4] A. Górski, J. Kruszyńska, K. Krzykwa, K. Lewandowska, M. Marczuk, M. Mierzejewski, P. Sątowska-Strycharczyk, Ł. Strycharczyk, Ł. Świątek, *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*. *Krótkie komentarze Becka*, red. M. Dyl, M. Królikowski, C.H. Beck, Warszawa 2021, s. 413–452.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

macji o transakcjach oraz ich udostępnianie, przekazywanie organom informacji, a także dokumentacji uzasadniających popełnienie przestępstwa oraz wymianę informacji z jednostkami współpracującymi. Zadaniem GIIF jest też sporządzanie krajowej oceny ryzyka prania pieniędzy i finansowania terroryzmu, a także ustalenie strategii przeciwdziałania. Katalog zawiera też takie zadania, jak: wydawanie decyzji w sprawach wpisu na listę osób i podmiotów, wobec których stosuje się szczególne środki ograniczające; współpraca z organami innych państw, a także zagranicznymi instytucjami i międzynarodowymi organizacjami, wymiana informacji z zagranicznymi jednostkami analityki finansowej; nakładanie kar administracyjnych, udostępnianie wiedzy i informacji z zakresu przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w Biuletynie Informacji Publicznej. GIIF powinien też inicjować inne zadania w celu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, czego przykładem może być zawieranie porozumień z podmiotami z sektora prywatnego w celu gromadzenia dodatkowych istotnych informacji. Wśród zadań wymieniono też właśnie przeprowadzanie procedury wstrzymania transakcji lub blokady rachunku[5]. W realizacji tych zadań ustawowych GIIF jest wspomagany przez Departament Informacji Finansowej Ministerstwa Finansów[6]. Wspólnie tworzą one jednostkę analityki finansowej, czyli agencję państwową odpowiedzialną za analizę i dalsze przekazanie organom ujawnionych informacji finansowych, gdy zachodzi jakiekolwiek podejrzenie wystąpienia czynu zabronionego lub po prostu krajowe przepisy przeciwdziałania praniu pieniędzy tego wymagają[7]. Rolę opiniodawczą i doradczą sprawuje działający przy GIIF Komitet Bezpieczeństwa Finansowego[8], który opiniuje krajową ocenę ryzyka, wydaje rekomendacje co do stosowania środków ograniczających, a także dokonuje ocen rozwiązań prawnych[9].

Poza zadaniami ustawowymi na Głównego Inspektora Informacji Finansowej nałożono również w art. 14 obowiązek przekazania Prezesowi Rady Ministrów, za pośrednictwem ministra właściwego do spraw finansów publicznych, rocznego sprawozdania ze swojej działalności. Powinno ono zawierać liczbę przekazanych przez instytucje oraz jednostki współpracujące informacji wraz z danymi statystycznymi, a także opis działań podjętych na ich podstawie. Liczbę postępowań karnych, jak i osób, które otrzymały zarzuty oraz zostały prawomocnie skazane za przestępstwa prania pieniędzy i finansowania terroryzmu. Sprawozdanie

[5] *Ibidem*.

[6] *Generalny Inspektor Informacji,* https://www.gov.pl/web/finanse/generalny-inspektor-informacji-finansowej (data dostępu: 1 września 2021).

[7] Konwencja Rady Europy z dnia 16 maja 2005 r. – o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu (Dz.U. z 2008 r., nr 165, poz. 1028).

[8] A. Sroga, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Obowiązki biur rachunkowych*. Infor, Warszawa 2021, s. 118–121.

[9] Generalny Inspektor Informacji Finansowej.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

zawiera też informację o wartościach majątkowych, w stosunku do których dokonano zamrożenia, wstrzymania transakcji i blokady lub orzeczono zajęcie, zabezpieczenie majątkowe lub przepadek, liczbie kontroli oraz kar administracyjnych, a także informacje o działalności Komitetu Bezpieczeństwa Finansowego.

Główny Inspektor Informacji Finansowej, jak już wspomniano wcześniej, posiada uprawnienia do blokady rachunku oraz wstrzymania transakcji. Może to zrobić z urzędu lub na wniosek instytucji obowiązanej, takiej jak: bank, zakład ubezpieczeń, fundusz inwestycyjny czy też spółdzielcza kasa oszczędnościowo-kredytowa, jednak jedynie wtedy, gdy zachodzi pojrzenie popełnienia przestępstwa[10]. W przypadku uzasadnionego podejrzenia instytucja zobowiązana ma obowiązek niezwłocznego powiadomienia GIIF za pomocą środków komunikacji elektronicznej oraz podania posiadanych przez siebie informacji i przewidywanej daty transakcji, a także dane identyfikacyjne, numer rachunku i rodzaj oraz wielkość wartości majątkowych. Inspektor potwierdza przyjęcie zgłoszenia urzędowym potwierdzeniem zawierającym dokładną datę i godzinę. Od tego czasu przez 24 godziny instytucja obowiązana nie przeprowadza transakcji czekając na dalsze polecenia GIIF, a ten, jeśli uzna, iż transakcja może mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, może wydać, z określeniem wartości objętych, żądanie blokady rachunku lub wstrzymania transakcji, jednak na nie dłużej niż 96 godzin od daty widniejącej na potwierdzeniu. Następnie niezwłocznie powiadamia prokuratora o podejrzeniu popełnienia przestępstwa. Po otrzymaniu żądania instytucja dokonuje blokady lub wstrzymania. Jednakże, jeśli GIIF uzna, iż posiadane informacje nie stanowią podstawy do podejrzenia popełnienia przestępstwa, może zwolnić instytucję z obowiązku nieprowadzenia transakcji w ciągu najbliższych 24 godzin, może zrobić to też, gdy uznania, że wstrzymanie transakcji lub blokada rachunku mogłyby utrudnić wykonywanie zadań organom wymiaru sprawiedliwości oraz służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw lub przestępstw skarbowych. Inspektor Generalny może powiadomić prokuratora o uzasadnionym popełnieniu przestępstwa nie tylko jeżeli otrzyma zgłoszenie z zewnątrz, ale też gdy informacje takie posiada z własnych analiz i przetwarzania danych[11].

Uprawnienie do blokady rachunku lub wstrzymania transakcji posiada również prokurator. Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wskazuje współpracę oraz przekaz informacji między prokuratorem a GIIF. Prokurator informuje inspektora o wydaniu postanowienia o blokadzie rachunku lub wstrzymaniu transakcji, wszczęciu postępowania, przedstawieniu zarzutu

[10] K. Kaseja, *Podmioty uprawnione do dokonania blokady rachunku lub wstrzymania transakcji*, z. 3, Krajowa Szkoła Sądownictwa i Prokuratury, Kraków 2018, s. 92.

[11] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

i wniesieniu aktu oskarżenia w terminie do 7 dni od dokonania danej czynności, wraz z podaniem okoliczności oraz danych identyfikacyjnych. Jak było wspomniane w poprzednim akapicie, przekazywanie informacji odbywa się w sposób obustronny. GIIF ma obowiązek niezwłocznego powiadamiania o podejrzeniu przestępstwa prokuratora, a ten może zablokować rachunek lub wstrzymać transakcję na czas oznaczony nie dłuższy niż 6 miesięcy. Obowiązek niezwłocznego informowania prokuratora o uzasadnionym podejrzeniu, iż wartości majątkowe będące przedmiotem transakcji lub zgromadzone na rachunku pochodzą z przestępstwa innego niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub z przestępstwa skarbowego albo mają związek z przestępstwem innym niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub z przestępstwem skarbowym, spoczywa również na instytucjach obowiązanych. Jednakże z wyłączeniem ustawowym banków krajowych, oddziałów banków zagranicznych, oddziałów instytucji kredytowych oraz spółdzielczych kas oszczędnościowo-kredytowych. W ciągu 96 godzin prokurator wydaje postanowienie o wszczęciu lub odmowie wszczęcia postępowania, o czym musi powiadomić instytucję. W pierwszym przypadku w drodze postanowienia dodatkowo dokonuje blokady rachunku lub wstrzymania transakcji na okres nie dłuższy niż 6 miesięcy licząc od dnia zawiadomienia. Jednakże jeśli w ciągu 6 miesięcy od wydania postanowienia nie dojdzie do wydania postanowienia o zabezpieczeniu majątkowym lub postanowienia w przedmiocie dowodów rzeczowych, wstrzymanie transakcji lub blokada rachunku upada. Prokurator posiada też uprawnienia do samodzielnego zastosowania blokady rachunku lub wstrzymania transakcji bez zawiadomienia od GIIF lub instytucji[12].

Na prokuratorze spoczywa też obowiązek, nałożony w art. 107 Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, dotyczący przekazania Głównemu Inspektorowi Informacji Finansowej w ciągu 30 dni od otrzymania zgłoszenia informacji o: wydaniu postanowienia w przedmiocie blokady rachunku lub wstrzymania transakcji; zawieszeniu postępowania; podjęciu zawieszonego postępowania; wydaniu postanowienia o przedstawieniu zarzutu popełnienia przestępstwa. Dzięki temu GIIF wie, iż prokurator podjął działania i zastosował blokadę, dzięki temu informacja jest rozprowadzona w całym „systemie" i żadne działania nie będą bezcelowe czy powtórzone.

W art. 88 wspomniano też o współpracy GIIF z Agencją Bezpieczeństwa Wewnętrznego (ABW). Inspektor niezwłocznie przekazuje informację o żądaniu wstrzymania transakcji lub blokady rachunku szefowi ABW za pomocą środków komunikacji elektronicznej. Obie te instytucje mają na celu walkę z praniem pieniędzy oraz przeciwdziałanie finansowaniu terroryzmu. Wskazanie sposobu przekazania informacji przez drogę elektroniczną ma pomóc w jak najszybszym przepływie informacji oraz podjęciu przez ABW odpowiednich działań. Współ-

[12] *Ibidem*.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

praca na tej płaszczyźnie jest ogromnie ważna ze względu na możliwy konflikt interesów obu podmiotów. Zabezpieczenie środków może być przedwczesne i negatywnie wpłynąć na czynności operacyjno-rozpoznawcze prowadzone przez służby. W szczególnych przypadkach, takich jak np. finansowanie terroryzmu GIIF może też wcześniej skonsultować się z ABW ze względu na odrębność prowadzonych działań[13].

Istotny jest również zapis w art. 113 Ustawy stanowiący o współpracy i przekazie informacji nie tylko w obrębie kraju, ale również i za granicą. GIIF może przekazać informacje lub dokumenty zagranicznej jednostce analityki finansowej wskazując przy tym, komu mogą być one udostępniane oraz do jakich celów wykorzystywane. Działa to również w przeciwną stronę, GIIF może wykorzystywać informacje i dokumenty pozyskane od zagranicznych jednostek analityki finansowej, ale jedynie w celach, jakie jednostka wyznaczy w zgodzie na ich użycie. Zgoda niezbędna jest również w przypadku chęci przekazania pozyskanych informacji sądom, jednostkom współpracującym lub innym jednostkom analityki finansowej lub na wykorzystanie takich informacji do celów innych niż wykonywanie swoich zadań. Należy zwrócić uwagę na jeszcze jeden istotny element współpracy. W przypadku podejrzenia popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, aby uprawdopodobnić to podejrzenie, zagraniczna jednostka analityki finansowej może zgłosić się do polskiego GIIF z wnioskiem o wydanie żądania ustanowienia blokady rachunku lub wstrzymania transakcji[14].

11.3. WSTRZYMANIE TRANSAKCJI I BLOKADA RACHUNKU W PRAWIE BANKOWYM

Ustawa z dnia 29 sierpnia 1997 r. prawo bankowe[15], podobnie jak wspomniana wcześniej Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, również wykorzystuje narzędzia, jakimi jest wstrzymanie transakcji oraz blokada rachunku. Ustawa prawo bankowe nie posiada własnych definicji legalnych dla sformułowań wstrzymanie transakcji oraz blokada rachunku, można więc wysnuć wniosek, iż są to te same środki co w poprzednio omawianej ustawie, jednakże zasady, na których mogą zostać one wykorzystane, oraz podmioty posiadające uprawnienia do ich użycia są inne.

Ustawowym obowiązkiem banku jest przeciwdziałanie wykorzystywaniu swojej działalności dla celów mających związek z przestępstwami prania pieniędzy

[13] M. Kędzierski, *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, s. 130.

[14] *Ibidem*.

[15] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 1997 r., nr 140, poz. 939).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

oraz finansowania terroryzmu. W obecnych czasach zważywszy na łatwy dostęp, między innymi internetowy, szybkość działania oraz niską cenę produktów bankowych są one częściej wykorzystywane do popełniania przestępstw finansowych. Bank ma obowiązek sprawować kontrolę i nadzór nad transakcjami oraz zgłaszać wszelkie podejrzenia i nieprawidłowości w trybie Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, do której odesłanie znajduje się w art. 106. Pracownikowi, który nie dopełni obowiązku i nie zgłosi okoliczności podejrzenia przestępstwa, grozi odpowiedzialność porządkowa, a nawet, jeśli wypełnia znamiona czynu, odpowiedzialność karna.

Poza tym, ustawodawca uregulował również kwestie powstania ewentualnej szkody. Jeśli bank wykona w dobrej wierze czynności mające na celu przeciwdziałanie wykorzystaniu swojej działalności dla celów mających związek z przestępstwem prania pieniędzy lub finansowania terroryzmu, nie ponosi odpowiedzialności za szkodę powstałą w takich okolicznościach. Jeżeli natomiast podczas dalszej analizy lub postępowania dojdzie do ustalenia, iż okoliczności budzące podejrzenia nie miały związku z przestępstwem ani ukrywaniem działań przestępczych, to odpowiedzialność za szkodę wynikającą ze wstrzymania czynności bankowych ponosi Skarb Państwa[16]. Stanowi to gwarancja z art. 77 ust. 1 Konstytucji[17]. Gwarantuje ona każdemu prawo do wynagrodzenia szkody wyrządzonej przez niezgodne z prawem działanie organu władzy publiczne. Jest to bardzo istotne, ponieważ postanowienie w przedmiocie blokady rachunku może spowodować potencjalnie bardzo wysoką szkodę materialną. Blokada na rachunku może rodzić wiele problemów dla właściciela rachunku, np., gdy prowadzi on działalność gospodarczą. Utrzymywanie blokady, a następnie zabezpieczenia majątkowego może prowadzić do problemów z regulowaniem zobowiązań, a tym samym do zadłużenia czy utraty płynności finansowej, a nawet upadłości[18]. W sytuacji gdy podejrzenia popełnienia przestępstwa okazują się nieprawdziwe, szkoda może zostać naprawiona.

Uzupełnieniem regulacji wykorzystania tych narzędzi do walki banku z przestępstwami finansowymi jest art. 106 a Ustawy prawo bankowe. Odnosi się on do sytuacji, w której zaistnieje uzasadnione podejrzenie, że działalność banku jest wykorzystywana w celu ukrycia działań przestępczych lub dla celów mających związek z przestępstwem skarbowym lub innym przestępstwem niż przestępstwo, o którym mowa w art. 165 a lub art. 299 Kodeksu karnego[19]. Innym przestępstwem wspomnianym w artykule może być:

[16] *Ibidem*.

[17] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483).

[18] M. Bergman, *Blokada środków na rachunku bankowym,* https://www.filipiakbabicz.com/przestepstwa-w-biznesie/2020/07/02/blokada-srodkow-na-rachunku-bankowym (data dostępu: 6 września 2021).

[19] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r., nr 88, poz. 553).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- przestępstwo oszustwa (art. 286 KK),
- przestępstwo oszustwa kredytowego (art. 297 KK),
- przestępstwo posługiwania się podrobionym dokumentem (art. 270 KK).

Pierwszym obowiązkiem banku w takiej sytuacji jest zawiadomienie prokuratora, policji lub innego organu uprawnionego do prowadzenia postępowania przygotowawczego, czyli np. ABW. Istotnym jest, iż zawiadomienie banku skierowane do prokuratora winno zawierać wszelkie informacje posiadane przez bank o transakcji, co do której istnieje podejrzenie. W tym zakresie nie obowiązuje tajemnica bankowa. Jest to ważne, ponieważ podejrzenie popełnienia przestępstwa musi być uzasadnione, a prokurator musi dysponować chociaż podstawowymi informacjami na temat zdarzenia, aby dokonać kwalifikacji prawnej czynu wydając postanowienie o wszczęciu postępowania przygotowawczego. Samo lakoniczne zawiadomienie banku bywa niewystarczające dla prokuratora, aby podjąć decyzję w przedmiocie wszczęcia postępowania i sformułować opis czynu[20].

Organ po otrzymaniu zgłoszenia może żądać uzupełnienia informacji, także w toku czynności podejmowanych na podstawie art. 307 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[21], więc wyłączone są dowody z opinii biegłego oraz te, które są połączone z koniecznością sporządzenia protokołu, z wyjątkiem przyjęcia ustnego zawiadomienia o przestępstwie lub wniosku o ściganie. Co istotne, uzupełnienie danych może odbyć się też w formie przesłuchania w charakterze świadka osoby składającej zawiadomienie o przestępstwie. Uprawnienie do żądania uzupełnienia informacji przysługuje prokuratorowi, policji lub innemu organowi właściwemu do prowadzenia postępowania przygotowawczego. W przypadku opisanym w art. 106 a ust. 2 prokurator nie musi już występować do właściwego sądu okręgowego z wnioskiem o wydanie postanowienia w przedmiocie zwolnienia z zachowania tajemnicy bankowej banku składającego zawiadomienie o możliwości popełnienia przestępstwa[22].

Kolejnym krokiem w przypadku uzasadnionego podejrzenia, iż środki zgromadzone na rachunku bankowym pochodzą w całości lub w części z działalności przestępczej lub mają związek z przestępstwem skarbowym lub przestępstwem innym niż przestępstwo prania pieniędzy lub finansowania terroryzmu, jest dokonanie przez bank blokady środków na rachunku, jednakże jedynie do wysokości kwoty, co do której zachodzi podejrzenie. Taka blokada może trwać nie dłużej niż 72 godziny. O dokonanej blokadzie bank ma obowiązek niezwłocznie zawiadomić prokuratora. Jest to czas dla prokuratora na wydanie postanowienia o wszczęciu lub odmowie wszczęcia postępowania przygotowawczego w związku z dokonanym

[20] K. Kaseja, *op. cit.,* s. 88.

[21] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. z 1997 r., nr 89, poz. 555).

[22] Ł. Krysiński, *Odkrywanie tajemnic kont bankowych,* „Prokuratura i Prawo" 2021, nr 4, s. 131.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

przez bank zawiadomieniem oraz powiadomienie banku o swojej decyzji[23]. W razie wszczęcia postępowania prokurator może, w drodze postanowienia, wstrzymać określoną transakcję lub dokonać blokady środków na rachunku na czas oznaczony, nie dłuższy niż 3 miesiące. W postanowieniu musi zostać określony dokładnie zakres, sposób i termin wstrzymania transakcji lub blokady środków na rachunku. Na postanowienie prokuratora w przedmiocie stosowania blokady środków na rachunku przysługuje zażalenie do sądu właściwego dla sprawy w terminie 7 dni[24].

W ustępie 3a art. 106a ww. ustawy ustawodawca określił postępowanie w przypadku uzasadnionego podejrzenia popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, albo wykorzystywania działalności banku w celu ukrycia działań przestępczych lub dla celów mających związek z przestępstwem lub przestępstwem skarbowym. W takim przypadku prokurator może, tak jak była o tym mowa w Ustawie o praniu pieniędzy oraz finansowaniu terroryzmu, w drodze postanowienia, wstrzymać określoną transakcję lub dokonać blokady środków na rachunku bankowym na czas oznaczony, nie dłuższy niż 6 miesięcy. Może to zrobić również w przypadku, gdy nie doszło do złożenia zawiadomienia, ale sam powziął informacje o podejrzeniu popełnienia przestępstwa spełniającego znamiona czynu[25].

Kolejnym podobieństwem do Ustawy o praniu pieniędzy oraz finansowaniu terroryzmu jest zapis ustawodawcy o upadku wstrzymana transakcji lub blokady rachunku, jeżeli przed upływem 3 miesięcy od złożenia zawiadomienia przez bank lub od wydania postanowienia przez prokuratora nie zostanie wydane postanowienie o zabezpieczeniu majątkowym lub postanowienie w przedmiocie dowodów rzeczowych[26].

Ustawodawca w art. 106 a zastosował również odesłanie. W przypadku kwestii nie uregulowanych ustawą właściwe są przepisy Kodeksu postępowania karnego.

Po analizie przepisów można stwierdzić, iż Ustawa prawo bankowe nadaje uprawnienia do blokady rachunku bankom oraz prokuratorowi, natomiast do wstrzymania transakcji jedynie prokuratorowi. W przypadku decyzji banku o blokadzie rachunku prokurator może środek ten zamienić na wstrzymanie transakcji lub zastosować oba narzędzia łącznie. Dodatkowo bank posiada samodzielną możliwość podjęcia decyzji o blokadzie tylko w przypadku wystąpienia przestępstwa skarbowego innego niż przestępstwo prania pieniędzy lub finansowania terroryzmu, jeżeli natomiast czyn wypełnia znamiona z art. 165a lub art. 299 Kodeksu karnego, decyzja ta nie leży po stronie banku, ale powiadomionego przez niego GIIF. Prawdopodobnie ustawodawca miał na celu istotność właściwego działania w przypadku tak poważnych przestępstw oraz nieingerowania banku w działania

[23] G. Sikorski, *Prawo bankowe, komentarz,* Warszawa 2015.

[24] *Ibidem*.

[25] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 1997 r., nr 140, poz. 939).

[26] *Ibidem*.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

operacyjne. Z drugiej strony jednak nadanie bankom uprawnień do wstrzymania transakcji pozwoliłoby na szybsze działanie, co również w przypadku podejrzeń prania pieniędzy lub finansowania terroryzmu jest istotne.

Wśród różnic między ustawami można wyróżnić też dostęp do informacji dla osoby uprawnionej. Prawo bankowe nie reguluje udzielenia przez bank osobie uprawnionej informacji o dokonaniu blokady rachunku lub wstrzymaniu transakcji, natomiast Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu przewiduje, iż na żądanie wydającego dyspozycję lub zlecenie przeprowadzenia transakcji lub posiadacza albo właściciela przedmiotowych wartości majątkowych instytucja obowiązana może poinformować go o wstrzymaniu transakcji lub blokadzie rachunku i wskazać organ, który tego zażądał[27].

W wielu publikacjach naukowych negatywnie oceniony został fakt, iż Ustawa Prawo bankowe nie wskazuje na żadne kryteria, zgodnie z którymi bank powinien uznawać poszczególne transakcje za podejrzane, a w konsekwencji podejmować decyzję o dokonaniu blokady środków na rachunku. Badacze wskazują na fakt, tego, że bank nie jest organem władzy publicznej i nie powinien mieć możliwości samodzielnej oceny i decydowania o wprowadzeniu blokady. Powołują konieczność powstania unormowania zawierającego w swym zapisie określone kryteria, zgodnie z którymi bank powinien oceniać związek konkretnej transakcji z przestępstwem lub przestępstwem skarbowym[28].

11.4. WYKORZYSTANIE PRZEZ PAŃSTWO BLOKADY RACHUNKU I WSTRZYMANIA TRANSAKCJI

Blokada rachunku oraz wstrzymanie transakcji stanowią narzędzie nadane przez ustawodawcę w celu skutecznego i szybkiego zwalczania prób popełniania przestępstw skarbowych. Najszerzej narzędzia te omówiono we wspomnianych już wcześniej Ustawie Prawo bankowe oraz w Ustawie o praniu pieniędzy oraz finasowaniu terroryzmu. Jednakże zostały one użyte też w kilku innych ustawach. Uprawnienie do wstrzymania transakcji oraz blokady rachunku posiada jedynie GIIF oraz prokurator. Dodatkowo uprawnienie do samodzielnego dokonania blokady rachunku przysługuje: opisanemu wcześniej bankowi, przewodniczącemu KNF, spółdzielczej kasie oszczędnościowo-kredytowej oraz szefowi KAS.

[27] K. Kaseja, *op. cit*., s. 89.
[28] *Ibidem*.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Ustawa z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym[29] nadaje uprawnienie do dokonania blokady rachunku Przewodniczącemu Komisji Nadzoru Finansowego (KNF) i jego zastępcy. Wskazane podmioty mogą wystąpić z żądaniem dokonania blokady wyłącznie wtedy, gdy powezmą uzasadnione podejrzenie, że transakcja, która została dokonana lub ma zostać dokonana, może mieć związek z popełnieniem przestępstwa nieuprawnionego wykorzystania informacji poufnej, przestępstwa nieuprawnionego udzielania rekomendacji lub nakłaniania do nabycia lub zbycia instrumentów finansowych, których dotyczy informacja poufna, lub przestępstwa manipulacji instrumentami finansowymi. W tej ustawie blokadę rachunku zdefiniowano jako „czasowe uniemożliwienie dysponowania i korzystania z całości lub części instrumentów finansowych lub środków pieniężnych zgromadzonych na rachunku, w tym również przez podmiot nadzorowany, z wyłączeniem dokonania rozliczeń w instrumentach finansowych lub środkach pieniężnych wynikających z transakcji zawartych i zobowiązań wynikających z nabytych instrumentów finansowych przed otrzymaniem żądania”[30]. Dodatkowo ustawa określa rodzaj rachunków, na których może zostać dokonana blokada: rachunek papierów wartościowych, rachunek zbiorczy, inny rachunek, na którym są zapisywane instrumenty finansowe niebędące papierami wartościowymi, oraz rachunek pieniężny. Okres, na jaki może zostać dokonana blokada rachunku, wynosi tylko 48 godzin.

Na mocy Ustawy z dnia 5 listopada 2009 r. wraz z jej późniejszymi zmianami o spółdzielczych kasach oszczędnościowo-kredytowych[31] uprawnienie do blokady rachunku posiada spółdzielcza kasa oszczędnościowo-kredytowa. Ma ona możliwość blokady na okres nie dłuższy niż 72 godziny, środków zgromadzonych na prowadzonym przez nią rachunku w przypadku wystąpienia uzasadnionego podejrzenia, że zgromadzone na tym rachunku środki w całości lub w części pochodzą z przestępstwa skarbowego albo przestępstwa innego niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub mają z nim związek. Dalszy tryb postępowania jest taki jak w Ustawie Prawo bankowe. W ustawie widnieje też zapis o przypadku powzięcia podejrzenia przestępstwa prania pieniędzy lub finansowania terroryzmu lub wykorzystywania działalności kasy w celu ukrycia działań przestępczych lub dla celów mających związek z przestępstwem lub przestępstwem skarbowym. W takiej sytuacji blokady rachunku lub wstrzymania transakcji dokonuje prokurator na okres nie dłuższy niż 6 miesięcy.

Po nowelizacji Ordynacji podatkowej[32] uprawnienia do wydania postanowienia o blokadzie rachunku podmiotu kwalifikowanego na okres nie dłuższy niż 72,

[29] Ustawa z dnia 29 lipca 2005 r. – o nadzorze nad rynkiem kapitałowym (Dz.U. z 2005 r., nr 183, poz. 1537).

[30] *Ibidem*.

[31] Ustawa z dnia 5 listopada 2009 r. – o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. z 2012 r., poz. 855).

[32] Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz.U. z 1997 r., nr 137, poz. 926).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

uzyskał Szef Krajowej Administracji Skarbowej, jeżeli posiadane przez niego informacje wskazują, że podmiot kwalifikowany może wykorzystywać działalność banków lub spółdzielczych kas oszczędnościowo-kredytowych do celów mających związek z wyłudzeniami skarbowymi lub do czynności zmierzających do wyłudzenia skarbowego, a blokada rachunku jest konieczna, aby temu przeciwdziałać. Po wydaniu przedmiotowego postanowienia szef KAS jest zobowiązany do przekazania bankowi lub spółdzielczej kasie oszczędnościowo-kredytowej żądania dokonania blokady rachunku[33].

Krajowa Ocena Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu[34] niejednokrotnie porusza tematykę wykorzystania blokady rachunku oraz wstrzymania transakcji. Po pierwsze, został tam umieszczony zapis, jakie organy i na jakich zasadach mogą dokonać blokady rachunku lub wstrzymania transakcji. W rozdziale dotyczącym najczęstszych metod prania pieniędzy wskazano blokadę rachunku jako przykład walki z tym zjawiskiem, np. była ona wykorzystywana jako metoda walki z podejrzeniem prania pieniędzy przy wykorzystywaniu m.in. walut wirtualnych, wobec czego GIIF prowadzi coraz więcej postępowań analitycznych[35].

Krajowa ocena ryzyka zawiera również statystykę ilości blokad rachunku oraz wstrzymania transakcji na lata 2016–2018 wynikających z przeprowadzonych postępowań analitycznych. W 2016 r. liczba wstrzymań transakcji wyniosła 22, w 2017 r. 21, natomiast w 2018 r. jedynie 15. Jeśli chodzi o blokady rachunku w 2016 r., odnotowano ich 325, w 2017 r. 351, natomiast rok później 302, przy czym należy zauważyć, iż w 2018 r. doszło do poprzedniej zmiany w Ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Aby informacja ta była komplementarna, należy zwrócić również uwagę na dane o sumarycznej kwocie wartości majątkowych przechowywanych na zablokowanych przez GIIF rachunkach lub łącznej wartości wstrzymanych transakcji. Suma wartości majątkowych zgromadzonych na zablokowanych rachunkach w 2018 r. wyniosła aż 430,6 mln zł, a w latach 2016 i 2017 odpowiednio: 171,3 oraz 140,6 mln zł. Natomiast suma wartości majątkowych będących przedmiotem wstrzymania transakcji wyniosła: 31,2 mln zł w 2016 r., 3,0 mln zł w 2017 r. oraz aż 116,7 mln zł w 2018 r. Jak można zauważyć w 2018 r. miał miejsce znaczy wzrost sumy wartości majątkowych zgromadzonych na zablokowanych przez GIIF rachunkach, a także sumy wartości majątkowych będących przedmiotem transakcji wstrzymanych przez GIIF. Istotnym jest, że ok. 57,8% sumy wartości majątkowych zgromadzonych na zablokowanych w 2018 r. przez GIIF rachunkach oraz ok. 59,0% sumy wartości

[33] K. Kaseja*, op. cit.,* s. 102.

[34] *Krajowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu*, https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu (data dostępu: 7 września 2021).

[35] *Ibidem*.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

majątkowych będących przedmiotem transakcji wstrzymanych w 2018 r. przez GIIF dotyczyło blokad rachunków i wstrzymania transakcji w ramach jednego postępowania analitycznego[36]. Interesująca jest również statystyka dotycząca wartości majątkowych, w stosunku do których dokonano blokad rachunku lub wstrzymania transakcji dla wszczętych postępowań karnych w latach 2017 i 2018 dla art. 165 a KK oraz art. 299 KK. W stosunku do przestępstwa prania pieniędzy wyniosła ona 304 740 zł w 2017 r. oraz 2 032 243 zł w 2018 r. Natomiast kwota dla przestępstwa finansowania terroryzmu w obydwu badanych latach wyniosła 0[37]. Na taki rozkład danych może wpływać fakt zmiany przepisów w 2018 r. Wzrost wartości majątkowych, w stosunku do których dokonano blokad rachunku lub wstrzymania transakcji może byś spowodowany tym, że dostęp do możliwości popełniania przestępstwa prania pieniędzy jest coraz większy zważywszy na większy dostęp do nowoczesnych rozwiązań technologii oraz szerzący się dostęp do Internetu, ale też wzrastającą wykrywalność przestępstw.

Odniesienia do blokady rachunku oraz wstrzymania transakcji jako narzędzia walki z praniem pieniędzy oraz finansowaniem terroryzmu można znaleźć również w Sprawozdaniach rocznych z działalności Generalnego Inspektora Informacji Finansowej[38]. Już we wstępie sprawozdania za 2020 rok możemy znaleźć informację o wzroście w zakresie liczby blokad rachunku o 4,8% w stosunku do roku poprzedniego. Rozdział 7 zawiera dokładne analizy z postępowań przeprowadzonych przez GIIF. W 2020 r. Główny Inspektor Informacji Finansowej wszczął 2257 postępowań analitycznych (o 10% mniej niż w roku poprzednim).) GIIF dokonał w 2020 r. 673 blokad rachunków, na których zgromadzono środki o łącznej wartości ok. 246,2 mln zł, a także wstrzymał 32 transakcje na łączną kwotę ok. 26,7mln zł. W tym z inicjatywy GIIF dokonano 300 blokad na łączną kwotę ok. 57,4 mln zł oraz wstrzymano 13 transakcji, które opiewały łącznie na ok. 2,4 mln zł. Poza tym 2020 r. GIIF zwrócił się z wnioskiem do zagranicznej jednostki analityki finansowej o wykorzystanie jej uprawnień w przedmiocie żądania blokady rachunku. W wyniku tej interwencji zostały zablokowane dwa rachunki zagraniczne na łączną kwotę ok. 13,8 mln zł[39]. Wskazane wyżej kwoty środków zablokowanych na rachunkach są szacunkowe, rzeczywista kwota tych środków może być wyższa przez wzgląd na specyfikę blokady rachunków, a mianowicie, podczas trwania blokady nałożonej przez GIIF środki w dalszym ciągu mogą wpływać na rachunki, natomiast nie mogą być wypłacane lub transferowane na inne rachunki.

[36] Dane statystyczne dostępne w *Krajowej ocenie ryzyka.*

[37] *Ibidem*.

[38] *Sprawozdania roczne z działalności Generalnego Inspektora Informacji Finansowej*, https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej (data dostępu: 10 września 2021).

[39] Dane statystyczne ze *Sprawozdania rocznego z działalności Generalnego Inspektora Informacji Finansowej.*

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Sprawozdanie roczne zawiera również dane ilościowe odnoszące się do wstrzymania transakcji i zablokowania rachunku, przeprowadzonych na żądanie GIIF. Analizując dane z lat 2017–2020 można zauważyć tendencję wzrostową. Liczba blokad rachunków w 2020 r. – wzrost o ok. 5,2% w stosunku do roku poprzedniego oraz o ok. 122,9% w porównaniu do 2018 r. W analizowanym okresie podobna tendencja utrzymywała się w przypadku liczby transakcji wstrzymanych przez GIIF. W 2018 r. wstrzymano 15 transakcji, 37 w 2019 r. oraz w 2020 r. 32. W ubiegłym roku najwięcej powiadomień GIIF skierował do Krajowej Administracji Skarbowej (ok. 160). Dla porównania policja (w tym CBŚ) otrzymała 130 takich powiadomień, a ABW 77[40], są to najczęściej powiadamiane przez GIIF organy również w przeciągu kilku wcześniejszych lat.

11.5. PODSUMOWANIE

Reasumując, blokada rachunku oraz wstrzymanie transakcji są jednymi z narzędzi wykorzystywanymi do walki z praniem pieniędzy oraz finansowaniem terroryzmu. Nie są one uregulowane jednolicie i uregulowania ich dotyczące znajdują się w różnych ustawach.

Założony na wstępie cel rozdziału został osiągnięty. Przeprowadzono analizę pojęć blokada rachunku oraz wstrzymanie transakcji na podstawie różnych aktów prawnych. Porównano unormowania zawarte w prawie bankowym, a także w Ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Zbadano występowanie narzędzi w innych aktach prawnych, a także dane statystyczne pozwalające na przybliżenie rzeczywistego ich użycia. Wykazano iż uprawnienie do samodzielnego stosowania narzędzi posiada kilka różnych podmiotów, jednakże zasady co do ich użycia i możliwości wykorzystania środka nie są tożsame. Analizując statystyki oraz częstość ich użycia w ciągu ostatnich kilku lat niewątpliwie odgrywają ogromną rolę w systemie walki z ML/FT w Polsce. Zarówno jeśli chodzi o blokadę rachunku, jak i o wstrzymanie transakcji można zauważyć silny wzrost ilości zastosowania, może to świadczyć o lepszej wykrywalności podejrzeń tych przestępstw oraz innych przestępstw finansowych. Ponadto znacznie częściej wykorzystywane są one w przypadku prania pieniędzy niż finansowania terroryzmu, będącego znacznie mniejszym problemem w naszym kraju.

Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu nadaje uprawnienia do wstrzymania transakcji oraz blokady rachunku Głównemu Inspektorowi Informacji Finansowej w odniesieniu do przestępstw prania pieniędzy oraz finansowania terroryzmu. Uprawnienia do użycia obu narzędzi na mocy tej

[40] *Ibidem*.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

samej ustawy ma również prokurator. Natomiast Ustawa Prawo bankowe nadaje uprawnienie do samodzielnego dokonania blokady bankowi. Poza nimi uprawnienia do blokady rachunku posiada jeszcze przewodniczący KNF, spółdzielcza kasa oszczędnościowo-kredytowa oraz szefowi KAS na mocy innych ustaw.

Wyposażenie wyżej wymienionych organów miało na celu skuteczniejszą walkę z praniem pieniędzy, finansowaniem terroryzmu oraz innymi przestępstwami skarbowymi. Możliwość samodzielnego decydowania organu wpływa na szybkość działania, a także większą wykrywalność, co jest istotne, zważywszy na rozwój technologii i tym samym ułatwienie popełniania przestępstw finansowych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Paweł Piotrowski
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 12.

PROBLEMATYKA EGZEKUCJI KAR ADMINISTRACYJNYCH NAKŁADANYCH NA PODSTAWIE USTAWY AML/CFT

12.1. UWAGI WPROWADZAJĄCE

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu jest nie tylko pewnym drogowskazem mówiącym, jak postępować w konkretnych przypadkach lub nie postępować, by nie narazić się na odpowiedzialność, w tym karną, związaną z praniem pieniędzy oraz finansowaniem terroryzmu.

W tej części należy skupić się nie nad samym faktem przesłanek do nałożenia kary administracyjnej, katalogiem kar, organem uprawnionym do nakładania kary administracyjnej i jej egzekucji. Tej ostatniej części, czyli egzekucji, zostanie poświęcona większa uwaga. Sama część nadkładania kar administracyjnych czy też samego katalogu nie wymaga większej analizy, gdyż problematyka objęta tą częścią nie wykazuje większej liczby zagadnień. Już często sama egzekucja budzi nie tylko niepokój, strach, niechęć, a wręcz nienawiść do tych organów[1].

Organy egzekucyjne będące na samym końcu postępowań często spotykają się z agresją w stosunku do nich i ich pracowników. Tu należy przypomnieć, że to nie one dokonywały kontroli i nie wydawały decyzji w toku całego postępowania.

[1] A. Górski, J. Kruszyńska, K. Krzykwa, K. Lewandowska, M. Marczuk, M. Mierzejewski, P. Sątowska-Strycharczyk, Ł. Strycharczyk, Ł. Świątek, *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz. Krótkie komentarze Becka*. red. M. Dyl, M. Królikowski, C.H. Beck, Warszawa 2021, s. 590–638.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Organy te zostały stworzone już tylko do przymusowego wykonania zleconych im zadań, zaś dłużnik, który dobrowolnie spełnił swoje świadczenie, nie będzie mieć z nimi styczności.

12.2. KARY ADMINISTRACYJNE

Na dzień dzisiejszy obowiązuje ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[2]. Mimo że omawiane artykuły ustawy w większości nie były nowelizowane, to organy uprawnione do przeprowadzania kontroli i wydania decyzji w sprawie nałożenia kary lub jej odstąpienia przy spełnieniu okoliczności określonych w ustawie, coraz częściej dokonują kontroli oraz w pełni wykorzystują swoje uprawnienia w tym zakresie, w tym egzekucji kar. Sprawa również była poruszana w raportach Najwyższej Izby Kontroli.

Przesłanki do nałożenia kary administracyjnej zostały określone w art. 147 ustawy. Jest to zamknięty katalog dotyczący instytucji obowiązanej, która nie dopełnia obowiązku:

- wyznaczenia osoby odpowiedzialnej za wykonanie obowiązków określonych w ustawie, o którym mowa w art. 8,
- sporządzania oceny ryzyka oraz jej aktualizacji, o którym mowa w art. 27 ust. 3
- przekazania na żądanie Generalnego Inspektora oceny ryzyka oraz innych informacji mogących mieć wpływ na krajową ocenę ryzyka, o którym mowa w art. 28
- stosowania środków bezpieczeństwa finansowego[3], o których mowa w:
  - art. 33,
  - art. 43 – w przypadkach wyższego ryzyka prania pieniędzy lub finansowania terroryzmu oraz w przypadkach, o których mowa w art. 44–46,
- dokumentowania zastosowanych środków bezpieczeństwa finansowego oraz wyników bieżącej analizy przeprowadzanych transakcji oraz wykazania na żądanie organów, o których mowa w art. 130, zastosowania odpowiednich środków bezpieczeństwa, o których mowa w art. 34 ust. 3,
- przechowywania dokumentacji, o którym mowa w art. 49 ust. 1 i 2,
- wprowadzenia wewnętrznej procedury instytucji obowiązanej, o którym mowa w art. 50,
- wprowadzenia procedury grupowej, o którym mowa w art. 51,

[2] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2021 r., poz. 1132 z późn. zm.).

[3] *Prawo bezpieczeństwa finansowego*, red. P. Sitek, M. Karpiuk, M. Sawicka, Wydział Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego, Olsztyn 2016, s. 339.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- zapewnienia udziału osób wykonujących obowiązki związane z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu w programach szkoleniowych, o którym mowa w art. 52,
- wdrożenia wewnętrznej procedury anonimowego zgłaszania naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, o którym mowa w art. 53,
- zachowania w tajemnicy faktu przekazania Generalnemu Inspektorowi lub innym właściwym organom informacji, o którym mowa w art. 54 ust. 1,
- przekazania lub udostępnienia informacji, o którym mowa w art. 72 lub art. 76,
- przekazania zawiadomień, o którym mowa w art. 74, art. 86 ust. 1 lub art. 90 ust. 1

– podlega karze administracyjnej.

Ustawodawca dość precyzyjnie określił przesłanki do nałożenia kar administracyjnych odwołując się do konkretnych przypadków określonych w tym samym akcie nie odwołując się do innych aktów prawnych.

Samo nałożenie kary administracyjnej za niedopełnienie obowiązków wynikających z przepisów unijnych zostało uregulowane w art. 148 o następującym brzmieniu

Instytucja obowiązana, która nie dopełnia obowiązku:

- zapewnienia, aby transferowi środków pieniężnych towarzyszyły informacje o płatniku lub odbiorcy, o którym mowa w art. 4–6 rozporządzenia 2015/847,
- wdrożenia skutecznych procedur pozwalających na wykrywanie brakujących informacji o płatniku lub odbiorcy, o których mowa w art. 7, art. 8, art. 11 i art. 12 rozporządzenia 2015/847,
- informowania Generalnego Inspektora o nieprzekazywaniu wymaganych informacji o płatniku lub odbiorcy lub o podjętych działaniach, o którym mowa w art. 8 rozporządzenia 2015/847,
- zachowania wszystkich otrzymanych informacji o płatniku i odbiorcy, które towarzyszą transferowi, o którym mowa w art. 10 rozporządzenia 2015/847,
- udzielania Generalnemu Inspektorowi informacji, o którym mowa w art. 14 rozporządzenia 2015/847,
- przechowywania dokumentacji, o którym mowa w art. 16 rozporządzenia 2015/847

– podlega karze administracyjnej.

Już w tym przypadku ustawodawca dokonał odwołania do innego aktu to jest rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006[4]. Rozporządzenie składające się z 69 artykułów i ponad 100 stron

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

tekstu określają, jak przepływy pieniędzy pochodzących z nielegalnych źródeł realizowane za pomocą transferów środków pieniężnych mogą szkodzić integralności, stabilności i wiarygodności sektora finansowego oraz stanowić zagrożenie dla rynku wewnętrznego Unii, jak również rozwoju międzynarodowego. Pranie pieniędzy, finansowanie terroryzmu i przestępczości zorganizowanej nadal stanowią poważny problem, którym należy się zająć na szczeblu Unii[5].

Działania przestępców i ich wspólników, podejmowane czy to w celu ukrycia pochodzenia dochodów z przestępstwa, czy też w celu przekazania środków pieniężnych na działalność przestępczą lub cele terrorystyczne, mogą stanowić poważne zagrożenie dla prawidłowego funkcjonowania, integralności i stabilności systemu transferu środków pieniężnych oraz dla zaufania do systemu finansowego jako całości[6]. Ze względu na skalę działań, jakie zostały podjęte, Unia Europejska miała zapewnić jednolite wdrożenie w całej Unii międzynarodowych standardów przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

Ustawodawca odwołując się do wyżej opisanego aktu miał spełnić wymogi postawione Rzeczypospolitej Polskiej jako państwu członkowskiemu.

Z kolei w art. 149 przewiduje nałożenie kary administracyjnej za niedopełnienie obowiązków w zakresie stosowania szczególnych środków ograniczających.

Instytucja obowiązana, która:

- nie dopełnia obowiązku stosowania szczególnych środków ograniczających, o których mowa w art. 117 ust. 1, lub obowiązku przekazywania Generalnemu Inspektorowi posiadanych informacji związanych z ich stosowaniem,
- nie dopełnia obowiązku zamrażania funduszy lub zasobów gospodarczych albo zakazu udostępnienia funduszy lub zasobów gospodarczych, określonego w art. 2 ust. 1, 2 i 3 rozporządzenia 881/2002, art. 3 ust. 1 i 2 rozporządzenia 753/2011 oraz art. 2 ust. 1 rozporządzenia 2580/2001,
- nie stosuje się do zakazu świadomego i celowego udziału w działaniach, których przedmiotem lub celem jest, bezpośrednio lub pośrednio, próba obejścia nakazu zamrożenia lub zakazu udostępnienia funduszy lub zasobów gospodarczych lub obowiązku informowania o obejściu tych nakazów i zakazów, określonego w art. 4 ust. 1 i 2 rozporządzenia 881/2002, art. 3 ust. 3 rozporządzenia 753/2011 oraz art. 3 rozporządzenia 2580/2001,
- nie dopełnia obowiązku niezwłocznego przekazania informacji, które ułatwiłyby zapewnienie zgodności z rozporządzeniem 881/2002, rozporządzeniem 753/2011 oraz rozporządzeniem 2580/2001, lub obowiązku współpracy z Gene-

[5] P. Sitek, *Polityka pieniężna Narodowego Banku Polskiego i Europejskiego Banku Centralnego w obliczu kryzysu finansowego i po kryzysi*e (w:) *Wpływ prawa Unii Europejskiej na gospodarkę i samorząd terytorialny państw członkowskich*, red. M. Ganczar, J. Król, M. Szewczak, Wydawnictwo Afinance, Łódź 2017.

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. W sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia Rozporządzenia (WE) nr 1781/2006.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ralnym Inspektorem w zakresie weryfikacji tych informacji, określonego w art. 5 ust. 1 rozporządzenia 881/2002, art. 8 ust. 1 rozporządzenia 753/2011 oraz art. 4 ust. 1 rozporządzenia 2580/2001,
- nie stosuje się do zakazu świadczenia usług finansowych określonego w art. 2 ust. 2 rozporządzenia 2580/2001

– podlega karze administracyjnej.

Tu ustawodawca odwołał się do Rozporządzenia Wykonawczego Komisji (UE) 2019/1883 z dnia 8 listopada 2019 r. zmieniającego po raz 307. Rozporządzenie Rady (WE) nr 881/2002 wprowadzające niektóre szczególne środki ograniczające skierowane przeciwko niektórym osobom i podmiotom związanym z organizacjami ISIL (Daisz) i Al-Kaida[7] oraz Rozporządzenia Rady (UE) nr 753/2011 z dnia 1 sierpnia 2011 r. w sprawie środków ograniczających skierowanych przeciwko niektórym osobom, grupom, przedsiębiorstwom i podmiotom w związku z sytuacją w Afganistanie, Rozporządzenia Rady (WE) nr 2580/2001 z dnia 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu.

12.3. KATALOG KAR ADMINISTRACYJNYCH

Katalog kar administracyjnych został określony w artykule 150 Ustawy. Katalog ten zawiera nie tylko same kary, lecz również opisuje ich wysokość i, co ważne, warunki odstąpienia od nałożenia kary administracyjnej.

1. Karami administracyjnymi są:
- publikacja informacji o instytucji obowiązanej oraz zakresie naruszenia przepisów ustawy przez tę instytucję w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych,
- nakaz zaprzestania podejmowania przez instytucję obowiązaną określonych czynności,
- cofnięcie koncesji lub zezwolenia albo wykreślenie z rejestru działalności regulowanej,
- zakaz pełnienia obowiązków na stanowisku kierowniczym przez osobę odpowiedzialną za naruszenie przez instytucję obowiązaną przepisów ustawy przez okres nie dłuższy niż rok,
- kara pieniężna.

[7] Rozporządzenie Wykonawcze Komisji (UE) 2021/1460 z dnia 9 września 2021 r. zmieniające po raz 322. rozporządzenie Rady (WE) nr 881/2002 wprowadzające niektóre szczególne środki ograniczające skierowane przeciwko niektórym osobom i podmiotom związanym z organizacjami ISIL (Daisz) i Al-Kaida.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

2. Karę pieniężną nakłada się do wysokości dwukrotności kwoty korzyści osiągniętej lub straty unikniętej przez instytucję obowiązaną w wyniku naruszenia albo – w przypadku gdy nie jest możliwe ustalenie kwoty tej korzyści lub straty – do wysokości równowartości kwoty 1.000.000 euro.

3. Karę pieniężną nakłada się na instytucje obowiązane, o których mowa w art. 2 ust. 1 pkt 1–5, 7–11, 24 i 25:

- w przypadku osoby fizycznej – do wysokości 20 868 500 zł,
- w przypadku osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej – do wysokości równowartości kwoty 5 000 000 euro albo do wysokości 10% obrotu wykazanego w ostatnim zatwierdzonym sprawozdaniu finansowym za rok obrotowy lub w ostatnim skonsolidowanym sprawozdaniu finansowym za rok obrotowy – w przypadku instytucji objętych skonsolidowanym sprawozdaniem finansowym grupy kapitałowej.

4. Ustalając rodzaj kary administracyjnej oraz wysokość kary, uwzględnia się:

- wagę naruszenia i czas jego trwania;
- zakres odpowiedzialności instytucji obowiązanej;
- możliwości finansowe instytucji obowiązanej;
- skalę korzyści osiągniętych lub strat uniknięty przez instytucję obowiązaną, jeżeli można te korzyści lub straty ustalić;
- straty poniesione przez osoby trzecie w związku z naruszeniem, jeżeli można je ustalić;
- stopień współpracy instytucji obowiązanej z organami właściwymi w sprawach przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
- uprzednie naruszenia przepisów ustawy przez instytucję obowiązaną.

5. W szczególnie uzasadnionych przypadkach, gdy:

- waga naruszenia przepisów ustawy jest znikoma, a instytucja obowiązana zaprzestała naruszania przepisów ustawy lub
- za to samo zachowanie prawomocną decyzją na instytucję obowiązaną została uprzednio nałożona kara administracyjna przez inny uprawniony organ administracji publicznej lub instytucja obowiązana została prawomocnie ukarana za wykroczenie lub wykroczenie skarbowe lub prawomocnie skazana za przestępstwo lub przestępstwo skarbowe i uprzednia kara spełnia cele, dla których miałaby być nałożona kara administracyjna

– organy, o których mowa w art. 151 ust. 1, mogą, w drodze decyzji, odstąpić od nałożenia kary administracyjnej.

Artykuł 154 ustawy określa Kary pieniężne nakładane na członka organu zarządzającego instytucji obowiązanej odpowiedzialnego za wykonanie obowiązków ustawowych. Przedstawia się to w sposób następujący.

- w przypadku stwierdzenia naruszenia przez instytucję obowiązaną obowiązków, o których mowa w art. 147 lub art. 148, organy, o których mowa w art. 151 ust. 1, mogą nałożyć na osobę, o której mowa w art. 6–8, odpowie-

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

działną za wykonanie obowiązków określonych w ustawie w czasie, w którym naruszono te przepisy, karę pieniężną do wysokości 1 000 000 zł,
- do nakładania kary, o której mowa w ust. 1, stosuje się odpowiednio przepisy art. 150 ust. 4 i 5 oraz art. 152.

Wspomniane raporty Najwyższej Izby Kontroli[8] od początku dogłębnie wykazywały mocne, jak i słabe punkty działania Generalnego Inspektora Informacji Finansowej (dalej GIIF), który stanowi główny element polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. GIIF (będący sekretarzem albo podsekretarzem stanu w Ministerstwie Finansów) jest powoływany i odwoływany przez Prezesa Rady Ministrów na wniosek ministra właściwego do spraw finansów publicznych po zasięgnięciu opinii ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych (o ile został wyznaczony przez Prezesa Rady Ministrów). Zadania GIIF są określone w ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. poz. 723, ze zm.). W realizacji swoich zadań ustawowych GIIF jest wspomagany przez Departament Informacji Finansowej Ministerstwa Finansów. GIIF wraz z departamentem jest uważany za jednostkę analityki finansowej, zdefiniowaną w przepisach Unii Europejskiej[9].

Już na podstawie raportu NIK z 2015 r. czyli jeszcze przed wejściem w życie nowej ustawy stwierdzono, że według ustaleń kontroli własnych oraz kontroli prowadzonych przez podmioty wymienione w art. 21 ust. 3 ustawy GIIF prowadził postępowania administracyjne w sprawie nałożenia kar pieniężnych na instytucje obowiązane, którym udowodniono naruszenie przepisów ustawy.

W GIIF wszczynał te postępowania po upływie od kilku do 17 miesięcy od daty zakończenia kontroli lub otrzymania informacji o wynikach kontroli. Jako przyczynę wydłużonego okresu podejmowania postępowań administracyjnych wskazano duże obłożenie pracą pracowników Wydziału Kontroli Departament Informacji Finansowej (dalej DIF) – jednostka organizacyjna w strukturze Ministerstwa Finansów utworzona w celu wspierania w wykonywaniu ustawowych zadań Generalnego Inspektora Informacji Finansowej. Pełni rolę jednostki analityki finansowej. DIF, którzy oprócz zadań związanych z prowadzeniem postępowań administracyjnych i egzekucją należności realizują także inne zadania Wydziału Kontroli.

Jak wyjaśniono w pierwszej kolejności rozpatrywane były sprawy zagrożone ryzykiem przedawnienia kary pieniężnej. Zdaniem NIK DIF powinien podjąć działania organizacyjne w celu skrócenia okresu podejmowania postępowań administracyjnych. Skuteczność DIF w nakładaniu kar pieniężnych ograniczała jakość materiałów pokontrolnych przekazywanych przez podmioty wymienione w art. 21

[8] Raport NIK *System Przeciwdziałania Praniu Pieniędzy oraz Finansowaniu Terroryzmu* KBF.410.009.00.201 nr ewid. 37/2016/P/15/013/KBF.

[9] www.gov.pl/web/finanse/generalny-inspektor-informacji-finansowe.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

ust. 3 ustawy. Na 19 umorzonych w okresie objętym kontrolą spraw, w siedmiu przypadkach umorzenie nastąpiło ze względu na błędnie zebrany materiał dowodowy[10].

Jak widać z przedstawionego raportu, GIIF[11] jako organ egzekucyjny nie wykazywał się szybkością we wszczęciu postępowań aż do ich zakończenia.

Na podstawie przepisów starej ustawy AML/CTF postępowania w sprawie nałożenia kar pieniężnych na instytucje obowiązane za nieprawidłowości w zakresie wypełniania obowiązków, o których mowa w art. 34a starej ustawy AML/CTF, prowadzone były zgodne z przepisami Kodeksu postępowania administracyjnego (dalej Kpa). Nakładanie kar pieniężnych należało do zadań GIIF.

Przy ustalaniu wysokości kary pieniężnej GIIF zgodnie z ustawą oraz nadanymi kompetencjami uwzględniał rodzaj, zakres naruszenia, dotychczasową działalność instytucji oraz jej możliwości finansowe. W 2018 r. GIIF na podstawie przepisów jeszcze starej ustawy AML/CTF przeprowadził 49 postępowań administracyjnych w sprawie nałożenia na instytucje obowiązane kar pieniężnych za nieprzestrzeganie przepisów ustawy. Na podstawie wyników własnych kontroli GIIF zrealizowano 8 postępowań, tj. ok. 16,33%, a 41 postępowań (ok. 83,67%) na podstawie wyników kontroli przeprowadzonych przez inne organy, o których mowa w art. 21 ust. 3 starej ustawy AML/CTF[12].

GIIF wydał w 2018 r. 49 decyzji administracyjnych, z czego 4 decyzjami umorzono prowadzone postępowania administracyjne oraz 13 decyzjami odstąpiono od nałożenia administracyjnej kary pieniężnej i poprzestano na pouczeniu.

Kary administracyjne mogą zostać wymierzone przede wszystkim instytucjom obowiązanym, tj. podmiotom, na które zostały na gruncie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu nałożone różne obowiązki, między innymi identyfikacji i oceny ryzyka prania pieniędzy oraz finansowania terroryzmu, czy obowiązek współdziałania z GIIF. Podmioty te zostały podzielone na grupy i należą do nich nie tylko duże przedsiębiorstwa w tym banki. Dodatkowo instytucjami obowiązanymi są również fundacje, stowarzyszenia, doradcy podatkowi.

Należy jednak wskazać, że nie tylko wyżej wskazane podmioty mogą podlegać odpowiedzialności. W przypadku stwierdzenia przez uprawniony organ naruszenia przez instytucję obowiązaną niektórych obowiązków może zostać nałożona na wskazane osoby fizyczne. Do tego grona należą członkowie zarządu instytucji obowiązanej odpowiedzialni za wykonywanie obowiązków w zakresie AML, kadra kierownicza wyższego szczebla odpowiedzialna za wykonywanie obowiązków

[10] NIK Wyniki kontroli KBF.410.009.00.201 nr ewid. 37/2016/P/15/013/KBF.

[11] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2018 r.

[12] P. Gołębiewski, *Wpływ AML na sektor usług rachunkowych*, Kortowski Przegląd Prawniczy, Uniwersytetu Warmińsko-Mazurskiego w Olsztynie, Olsztyn 2019, s. 50–79.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

określonych w ustawie, pracownicy zajmujący kierownicze stanowiska, odpowiedzialni za zapewnienie zgodności działalności instytucji obowiązanej oraz jej pracowników z przepisami AML.

Katalog naruszeń, za które może zostać nałożona kara administracyjna, jest bardzo szeroki. Ustawa o AML dzieli je na trzy opisane wyżej kategorie, tj. niedopełnienie w artykułach 147–149 ustawy. Można wyróżnić trzy główne przypadki:

- obowiązków w zakresie przepisów ustawy,
- obowiązków w zakresie przepisów unijnych,
- obowiązków w ramach stosowania środków ograniczających.

Największe i najszersze znaczenie ma grupa pierwsza. Jest to spowodowane większą ilością obowiązków nałożonych na instytucje obowiązane. Nawet te najbardziej podstawowe, tj. wyznaczenie osoby odpowiedzialnej, sporządzanie oceny ryzyka oraz jej okresowa aktualizacja, wprowadzenie wewnętrznej procedury postępowania czy przekazywanie zawiadomień o podejrzanych transakcjach.

12.4. RODZAJ KARY

Ustawa o AML w przypadku wszystkich trzech wskazanych wyżej grup niedopełnienia obowiązków odnosi się do pojęcia grożącej kary administracyjnej. Jest to pojęcie zdefiniowane przez ustawodawcę, a rozumie się przez nie:

- publikację informacji o instytucji obowiązanej oraz zakresie naruszenia przepisów ustawy przez tę instytucję w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych,
- nakaz zaprzestania podejmowania przez instytucję obowiązaną określonych czynności,
- cofnięcie koncesji lub zezwolenia albo wykreślenie z rejestru działalności regulowanej,
- zakaz pełnienia obowiązków na stanowisku kierowniczym przez osobę odpowiedzialną za naruszenie przez instytucję obowiązaną przepisów ustawy, przez okres nie dłuższy niż rok,
- karę pieniężną.

Karę pieniężną nakłada się do wysokości dwukrotności kwoty korzyści osiągniętej lub straty unikniętej przez instytucję obowiązaną w wyniku naruszenia albo – w przypadku gdy nie jest możliwe ustalenie kwoty tej korzyści lub straty – do wysokości równowartości kwoty 1 000 000 euro.

Wskazana kara została podniesiona w stosunku do wcześniej obowiązujących regulacji dotyczących AML/CFT, w których wynosiła ona 750 000 zł.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Ustawodawca postanowił, żeby wysokość kar była wysoka, a co za tym idzie rażąca dla przedsiębiorców oraz osoby zagrożonych tego typu karą. Zwrócić należy uwagę, że kara pieniężna jest jedną z kilku rodzajów kar możliwych do zastosowania.

Przykładem może być kara polegająca na samej publikacji o naruszeniu przepisów, co może mieć dla przedsiębiorcy większe negatywne skutki niż uiszczenie kary administracyjnej. Podanie do publicznej informacji może skutkować zaprzestaniem współpracy z obecnymi kontrahentami oraz może zniechęcić nowych kontrahentów do współpracy nie tylko ze względu na dobro wspólnego niewspierania terroryzmu czy też prania pieniędzy, lecz skutkiem ubocznym może być postrzeganie ich instytucji jako wspierającej prawnie zabronione działania, czyli mogą pojawiać się negatywnie skutki, które mogą wpłynąć na wiarygodność danego przedsiębiorcy.

Kolejną rażącą karą jest np. cofnięcie koncesji. Cofnięcie koncesji powoduje, że dany przedsiębiorąca od momentu jej odebrania nie może wykonywać działalności co może skutkować natychmiastową eliminacją z rynku, co w połączeniu z karą pieniężną doprowadzi do całkowitego wykluczenia instytucji z funkcjonowania.

12.5. CZYNNIKI MAJĄCE WPŁYW NA WYSOKOŚĆ KARY

Decyzja co do wysokości nałożonej kary nie jest całkowicie arbitralna. Przepisy ustawy przewidują wiele przesłanek, które uprawniony organ musi wziąć pod uwagę przy jej wymiarze. Ustalając rodzaj kary administracyjnej oraz wysokość kary zarówno dla instytucji obowiązanych, jak i osób odpowiedzialnych, o których była wyżej mowa. Pominięcie któregokolwiek może stanowić podstawy do odwołania się od tej decyzji. W takim przypadku ustawa wskazuje następujące czynniki:

- wagę naruszenia i czas jego trwania;
- zakres odpowiedzialności instytucji obowiązanej,
- możliwości finansowe,
- skalę korzyści osiągniętych lub strat unikniętych przez instytucję obowiązaną, jeżeli można te korzyści lub straty ustalić,
- straty poniesione przez osoby trzecie w związku z naruszeniem, jeżeli można je ustalić,
- stopień współpracy z organami właściwymi w sprawach przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu,
- uprzednie naruszenia przepisów ustawy.

Jak wspomniano już wcześniej w szczególnie uzasadnionych przypadkach organ w drodze decyzji może nawet odstąpić od wymierzenia kary. Są to sytuacje, gdy

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

waga naruszenia przepisów ustawy jest znikoma, a instytucja obowiązana zaprzestała naruszania przepisów ustawy lub za to samo zachowanie prawomocną decyzją na instytucję obowiązaną została uprzednio nałożona kara administracyjna przez inny uprawniony organ administracji publicznej lub instytucja obowiązana została prawomocnie ukarana za wykroczenie lub wykroczenie skarbowe lub prawomocnie skazana za przestępstwo lub przestępstwo skarbowe i uprzednia kara spełnia cele, dla których miałaby być nałożona kara administracyjna.

12.6. EGZEKUCJA I ICH RODZAJE

W polskim prawie mamy dwa rodzaje egzekucji. Są to egzekucja sądowa i egzekucja administracyjna.

Egzekucja sądowa znajduje swoją podstawę w ustawie z dnia 17 listopada 1964 r. Kpc. Przyjmuje się, że sprawa egzekucyjna jest w istocie sprawą cywilną, tyle że ściśle sprawę cywilną należy odnosić do postępowania rozpoznawczego, a sprawę egzekucyjną do postępowania egzekucyjnego. Jego celem jest przymusowe zrealizowanie praw lub obowiązków ze stosunków cywilnoprawnych, a więc prawa cywilnego materialnego. Podstawą wszczęcia tego postępowania jest tytuł wykonawczy. Może zostać wszczęta na wniosek wierzyciela, prokuratora albo organizacji pozarządowej lub przez sąd z urzędu ze względu na rodzaj zobowiązania.

W przypadku omawianej ustawy będziemy mieli jednak styczność z egzekucją administracyjną. Egzekucja ta to zespół czynności podejmowanych przez organ egzekucyjny, wobec zobowiązanego, a także innych uczestników postępowania, które zostały podjęte w celu ostatecznego urzeczywistnienia norm prawa materialnego. Celem tego postępowania jest wyegzekwowanie od dłużnika zachowania zgodnego z treścią nałożonego na niego obowiązku. Organ egzekucyjny wszczyna egzekucję administracyjną na wniosek wierzyciela i na podstawie wystawionego przez niego tytułu wykonawczego.

Nadany tytuł egzekucyjny stanowi dokument urzędowy, z którego musi wynikać kto jest wierzycielem, a kto dłużnikiem, oraz określać wysokość roszczenia. Podstawą postępowania mogą być również zobowiązania niepieniężne[13]. Wszelkie dane na temat stron sporu, a także określające wartości kwot podlegających postępowaniu muszą być szczegółowo wskazane, tak aby organ egzekucyjny nie miał żadnych wątpliwości, dlatego zawiera dokładne dane dłużnika jak imię i nazwisko lub nazwę firmy zobowiązanego i jej adres, a także numer identyfikacji podatkowej NIP, numer PESEL w przypadku osób fizycznych, treść podlegają-

[13] M. Staniszewski, *Egzekucja administracyjna obowiązków o charakterze niepieniężnym,* „Studia Administracyjne" 2018, nr 10, s. 33–50.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

cego egzekucji obowiązku, podstawę prawną tego obowiązku oraz stwierdzenie, że obowiązek jest wymagalny, a w przypadku egzekucji należności pieniężnej – także określenie jej wysokości, terminu, od którego nalicza się odsetki z tytułu niezapłacenia należności w terminie, oraz rodzaju i stawki tych odsetek, wskazanie zabezpieczenia należności pieniężnej hipoteką przymusową albo przez ustanowienie zastawu skarbowego lub rejestrowego, lub zastawu nieujawnionego w żadnym rejestrze, ze wskazaniem terminów powstania tych zabezpieczeń oraz numer rachunku, na który organ egzekucyjny ma przekazać należności w przypadku świadczenia pieniężnego[14].

W polskim prawie mamy do czynienia z dwoma rodzajami egzekucji w administracji. Pierwszy z nich to należności o charakterze pieniężnym, zaś drugi o charakterze niepieniężnym.

Postępowanie egzekucyjne na podstawie art. 56 ustawy o postępowaniu egzekucyjnym w administracji podlega zawieszeniu w całości lub w części m.in. w przypadku w razie wstrzymania wykonania, odroczenia terminu wykonania obowiązku albo rozłożenia na raty spłat należności pieniężnej, w razie śmierci zobowiązanego, jeżeli obowiązek nie jest ściśle związany z osobą zmarłego, w razie utraty przez zobowiązanego zdolności do czynności prawnych i braku jego przedstawiciela ustawowego, na żądanie wierzyciela[15].

Na podstawie art. 59 ustawy o postępowaniu egzekucyjnym w administracji „postępowanie egzekucyjne umarza się w całości albo w części w przypadku niedopuszczalności egzekucji administracyjnej, w tym ze względu na zobowiązanego, niewykonalności obowiązku o charakterze niepieniężnym, niespełnienia w tytule wykonawczym wymogów określonych w art. 27 elementy tytułu wykonawczego, śmierci zobowiązanego, gdy obowiązek:

- jest ściśle związany ze zobowiązanym,
- nie jest ściśle związany ze zobowiązanym, a egzekucja jest prowadzona wyłącznie z prawa majątkowego, które wygasło wskutek śmierci zobowiązanego,
- gdy postępowanie egzekucyjne zawieszone na żądanie wierzyciela nie zostało podjęte przed upływem 12 miesięcy od dnia zgłoszenia tego żądania,
- gdy z wnioskiem o umorzenie postępowania egzekucyjnego wystąpi wierzyciel,
- gdy odrębne ustawy tak stanowią".

[14] P. Gołębiewski, *Ramy prawne blokady rachunku bankowego i wstrzymania transakcji płatniczej* (w:) *Pieniądz i jego oddziaływanie na otoczenie*, red. P. Sitek, recenzowana praca zbiorowa, Elpil Druk Cyfrowy, Warszawa 2016, s. 155–193.

[15] S. Firkowski, *Zmiany w postępowaniu egzekucyjnym w administracji,* C.H. Beck, Warszawa 2020 s. 105–111.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

12.7. PO CO JEST EGZEKUCJA I KTO MOŻE PROWADZIĆ POSTĘPOWANIE

Egzekucja administracyjna obowiązków wymienionych powyżej jest możliwa wyłącznie na podstawie decyzji, postanowień lub orzeczeń wystawionych przez właściwe organy, a w przypadku organów administracji publicznej wynika z przepisów prawa.

Zgodnie z przepisami prawa możliwe jest prowadzenie egzekucji administracyjnej z obowiązków pieniężnych lub niepieniężnych, do których zaliczają się prawa majątkowe, ruchomości i nieruchomości. Od rodzaju prowadzonej egzekucji administracyjnej zależy, który organ będzie prowadził czynności egzekucyjne.

Organami uprawnionymi do prowadzenia egzekucji administracyjnej z obowiązków pieniężnych są:

- naczelnik Urzędu Skarbowego,
- właściwy organ gminy o statusie miasta oraz gminy wchodzącej w skład powiatu warszawskiego,
- przewodniczący organu orzekającego w sprawach o naruszenie dyscypliny finansów publicznych w pierwszej instancji,
- dyrektor oddziału Zakładu Ubezpieczeń Społecznych wyznaczony przez ministra właściwego do spraw finansów publicznych,
- dyrektor oddziału regionalnego Agencji Mienia Wojskowego,
- inny organ w zakresie określonym odrębnymi przepisami prawa.

Organami uprawnionymi do prowadzenia egzekucji administracyjnej z obowiązków niepieniężnych są:

- wojewoda,
- właściwy organ jednostki samorządu terytorialnego,
- kierownik wojewódzkiej służby, inspekcji lub straży,
- kierownik powiatowej służby, inspekcji lub straży,
- każdy organ Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu lub Straży Granicznej, prezes Urzędu Ochrony Danych Osobowych, organ Państwowej Inspekcji Pracy,
- inne organy powołane do ochrony spokoju i bezpieczeństwa.

Wszystkie wymienione organy administracyjne zajmują się egzekucją administracyjną ze względu na rodzaj zobowiązania dłużnika, czyli zobowiązanego. Dłużnik jako zobowiązany nie wykonując prawomocnej decyzji naraża się na ich działanie. Sam fakt, że dłużnik wiedząc o swoim zobowiązaniu i unikając np. spłaty w przypadku nałożenia na niego kary pieniężnej doprowadza do sytuacji w której będzie musiał liczyć się z dodatkowymi kosztami, czyli kosztami postępowania egzekucyjnego. Nie jest to tylko opłata egzekucyjna, która ma być swoistą

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

dodatkową karą dla dłużnika za niewykonanie dobrowolnego zobowiązania lecz też koszty biegłych. Dłużnicy często doprowadzają do samego postępowania nie dlatego, że nie mają środków pieniężnych, tylko są to celowe działania, gdyż nie zgadzają się z ich orzeczeniem lub wysokością, a nie działali w postępowaniu i np. nie składali odwołania lub innych środków zaskarżenia przewidzianych w ustawie.

Bez względu na fakt, czy jest to postępowanie prowadzone przez organy sądowe czy też administracyjne na odrębnych przepisach, należy stwierdzić, że mają one podobne efekty oraz trudności w ich prowadzeniu. Główną trudnością w prowadzeniu postępowań jest czas, w jakim organ jest w stanie wszcząć, prowadzić postępowanie oraz zakończyć je lub umorzyć wobec stwierdzenia bezskuteczności.

Czas jest często miernikiem wydajności systemu egzekucji[16]. Pod tym pojęciem ukryta jest też wydajność ludzka czy też niespodziewane przeszkody. Tu najlepszym przykładem jest często poruszana nie tylko w artykułach, wywiadach, a nawet w książkach światowa pandemia. Należy pamiętać, że pod pojęciem organu egzekucyjnego ukryte są osoby fizyczne, które dzięki wsparciu nowoczesnych technologii IT integrujących różne technologie służące pozyskiwaniu informacji, selekcjonowaniu jej, analizowaniu, przetwarzaniu, przechowywaniu, zarządzaniu.

Nowoczesna technologia służy za wsparcie tych ludzi, a nie wykonywanie za nich pracy. Z drugiej strony już samo postępowanie egzekucyjne rodzi już samo w sobie dużą ilość emocji, niestety, najczęściej są to emocje negatywne, które skierowane są do organów egzekucyjnych oraz ich pracowników. Organy te są postrzegane przez społeczeństwo nie tylko jako osoby bogacące się na krzywdzie ludzi, osoby nieempatyczne lecz jako „ślepe narzędzia" do wykonywania egzekucji. W postępowaniu sądowym mamy do czynienia nie tylko z dłużnikiem, ale również wierzycielem. Takim wierzycielem może stać się każdy z nas, każdy, kto będzie wymagał jak najszybszego i skutecznego działania w jego imieniu. W postępowaniu administracyjnym wierzycielem jest skarb państwa.

Zgodnie z art. 155 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2021 r. poz. 1132 z późn. zm.) wpływy z kar pieniężnych stanowią dochód budżetu państwa. Tu może pojawić się opinia, że może to stanowić aparat do, jak to często jest określane, zmniejszania „dziury w budżecie" państwa. Z drugiej strony ustawa przewiduje kary nie tylko finansowe. W tym momencie już słychać głos ludzi, by te kary były przeznaczone na inne ważne cele. Tylko by tam trafiły, muszą stanowić dochód skarbu państwa. Następnie członkowie rządu muszą uzgodnić, czy w danym roku jednym z priorytetów rządu będzie np. zapewnienie środków dla rodzin. Gdy wspólne stanowisko zostaje uzgodnione i spodziewane wpływy do budżetu zostaną rozdysponowane pomiędzy poszczególne resorty, ustawa trafia do Sejmu, stamtąd do Senatu i na

[16] P.M. Głąba, *Prawo jednostki do rozpoznania sprawy administracyjnej bez nieuzasadnionej zwłoki*, Admin. 2011, nr 1, s. 49–74.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

koniec do prezydenta. Gdy ten ustawę podpisze, jest ona obligatoryjną wytyczną do realizacji wydatków budżetu państwa[17].

Często działania organów egzekucyjnych doprowadza się do tego, że nie tylko ten sam organ jest nielubiany, lecz pogłębia się kwestia braku zaufania nie tylko do organu egzekucyjnego, lecz do całego systemu prawa[18].

Zasada pogłębienia zaufania uczestnika postępowania do władzy publicznej oraz jawności postępowań są to pryncypialne zasady ustalone w Kodeksie postępowania administracyjnego oraz Kodeksie postępowania cywilnego (dalej Kpc). Na uczestnika postępowania nałożone są na niego tylko obowiązki lecz również i prawa. Mając tu na myśli także prawo do prawidłowego informowania i pouczania. Tego typu zachowania mają na celu nie tylko szybkie zakończenie postępowania, lecz również ukazanie uczestnikowi postępowania, że jego prawa i uprawnienia są respektowane przez organy władzy publicznej.

Cel ten natomiast osiągnięty może być tylko przy przestrzeganiu wielu innych zasad zapisanych nie tylko w Kpa i Kpc, ale również w samej Konstytucji. Zasada zaufania obywateli do organów państwa uznawana jest za klamrę, która spina całość ogólnych zasad postępowania, jest to bowiem zasada najszersza pod względem zakresu. Można w niej pomieścić bogaty katalog zasad ogólnych, niewątpliwie bowiem pogłębianiu zaufania obywateli do organów państwa służy podejmowanie wszelkich działań niezbędnych do dokładnego wyjaśnienia stanu faktycznego, uwzględnianie interesu społecznego i słusznego interesu obywateli, udzielanie należytej i wyczerpującej informacji, zapewnienie stronom czynnego udziału na każdym etapie postępowania administracyjnego, jak i postępowania sądowego mającego na celu wyjaśnianie zasadności przesłanek, którymi organ kieruje się przy jego załatwianiu[19].

Wracając do tematyki egzekucji – jej głównymi sposobami są egzekucje skierowane do rachunków bankowych, wynagrodzenia za pracę, świadczeń emerytalno-rentowych, wierzytelności, ruchomości, nieruchomości. Ostatni sposób egzekucji jest używany często jako ostateczny ze względu na czas oraz koszty egzekucji tego majątku. Głównymi dodatkowymi kosztami są koszty związane z wyceną, czyli biegłych, ogłoszeń prasowych itp. Ograny egzekucyjne czy są organami sądowymi, czy administracyjnymi, w pierwszej kolejności przy wszczęciu postępowania prowadzą egzekucję papierową. Takie pojęcie często pojawia się i oznacza prowadzenie postępowań za pośrednictwem odpowiednich narzędzi IT do szybkiej wymiany informacji w celu szybkiego zakończenia postępowania. Często fizyczny

[17] www.gov.pl/web/finanse/budzet-panstwa.

[18] P. Gołębiewski, *System przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w Polsce* (w:) *Wyzwania i szanse dla polskiego sektora bankowego*, red. P. Sitek, recenzowana praca zbiorowa, Elpil Druk Cyfrowy, Warszawa 2016, s. 97–126.

[19] Wyrok WSA w Warszawie z dnia 8 grudnia 2010 r., VIII SA/Wa 640/10, publ. LEX nr 760393.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

kontakt z dłużkiem w postaci czynności w miejscu jego zamieszkania jest bezcelowy i wnoszący tylko jeszcze większe negatywne odczucia.

Organy egzekucyjne mają dostęp do różnych informacji oraz instytucji, tj. możliwość złożenia szybkiego zapytania do np. systemu OGNIVO, Zakładu Ubezpieczeń Społecznych (dalej ZUS), Centralnej Ewidencji Pojazdów i Kierowców (dalej CEPIK).

Już w 2007 r. powstała aplikacja OGNIVO, opracowana przez KIR, która umożliwiła szybką wymianę informacji pomiędzy uczestnikami systemów rozliczeniowych oraz instytucjami, takimi jak: ZUS, Poczta Polska, urzędy skarbowe, izby celne oraz organy sprawiedliwości.

W przypadku organów egzekucyjnych aplikacja umożliwia rozesłanie informacji o dłużniku czy posiada on rachunek bankowy w danym banku. Po uzyskaniu odpowiedzi zwrotnej organ egzekucyjny za pomocą tego samego systemu dokonuje już zajęcia, potocznie blokady, rachunku w konkretnym banku (centrali).

Takie rozwiązanie przyspiesza proces ustalania rachunków bankowych nawet o kilka miesięcy. Dodać należy, że system jest przez cały czas aktualizowany o wszystkie banki w tym banki spółdzielcze.

Wspomniany dostęp organów egzekucyjnych do ZUS daje szybką możliwość weryfikacji nie tylko danych dłużnika, ale również ustalenia jego głównego źródła utrzymania, czyli pracodawcy. Szybki dostęp do tych informacji ma wpływ na zajęcie wynagrodzenia. Tu należy wspomnieć o tym, że prawa dłużnika nie mogą być pominięte i egzekucja nie może być skierowana do kwot wolnych od egzekucji. Jest to swoiste zabezpieczenie podstawowych potrzeb życiowych dłużnika. Taki przypadek nie dotyczy egzekucji przeciwko osobie prawnej, która nie jest w ten sposób chroniona, i egzekucja nie tyle z wynagrodzenia, lecz z rachunku bankowego nie ma ograniczeń kwotowych.

Do kolejnych najczęściej stosowanych rodzajów egzekucji należy jej skierowanie do ruchomości dłużnika. Taki rodzaj egzekucji jest często używany przez organy egzekucyjne. W momencie fizycznego kontaktu organu z dłużnikiem często dochodzi np. do zajęcia pojazdów mechanicznych, ruchomości w postaci mebli, obrazów itp. Tego typu działania mają na celu również przymuszenie dłużnika do spłaty swojego zadłużenia, gdyż widzi on już realne zagrożenie utraty części majątku. Samo zajęcie tych ruchomości stanowi podstawę do wyznaczenia ich licytacji. Dłużnicy często nie udostępniają ich na wezwanie organu, co z jednej strony wydłuża postępowanie, lecz nie stanowi skutecznej ucieczki i ukrywania majątku.

CEPiK to rejestr prowadzony przez MSWiA, jest to baza kierowców i pojazdów zarejestrowanych na terenie Rzeczypospolitej Polskiej. Organ egzekucyjny w prostym, szybkim i elektronicznym zapytaniu może nie tylko dowiedzieć się, czy dłużnik jest właścicielem pojazdu, ale też ustalić ewentualnych współwłaścicieli, dane pojazdu, w tym, czy posiada aktualne badanie techniczne oraz obowiązkowe ubezpieczenie komunikacyjne jak i dane o historii pojazdu.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Jeżeli wyżej opisany katalog rodzajów egzekucji nie przyniósł efektów lub wartość świadczenia do spełniania jest wysoka, organ egzekucyjny stosuje kolejny sposób, czyli egzekucję z nieruchomości.

Ten rodzaj budzi wiele emocji. Powód jest oczywisty, gdyż głównie dotyczy nieruchomości mieszkalnych. Egzekucja z tego majątku jest procesem długim. Jest to spowodowane wysoką starannością i dokładnością między innymi w oszacowaniu nieruchomości i skuteczności doręczeń korespondencji.

Ten rodzaj egzekucji od pewnego okresu budzi emocje nie tylko u dłużników lecz u ewentualnych nabywców. Galopujące ceny nieruchomości oraz utrzymująca się inflacja skłania do inwestowania w nieruchomości, nie tylko w celach zarobkowych, lecz celu lokaty pieniędzy.

12.8. PODSUMOWANIE

Egzekucja kar administracyjnych to często niepotrzebny środek stosowania przymusu w celu wykonania decyzji administracyjnej. Wykazane liczne organy uprawnione do prowadzenia tych postępowań borykają się nie z dużą ilością spraw, a w przypadku spraw prowadzonych na podstawie omawianej ustawy jest ich coraz więcej, a poruszana problematyk jest specyficzna. Należy jednak pamiętać, że każdy obowiązek wynikający z przepisów prawa dotyczący należności pieniężnych lub niepieniężnych w sytuacji jego niespełnienia będzie podlegał egzekucji administracyjnej przez właściwy do tego organ administracji oraz uzyskanie tytułu egzekucyjnego wraz z wnioskiem wierzyciela staje się podstawą wszczęcia tego postępowania. Dobrowolne niepoddanie się obowiązkom wynikającym z nałożonej na dłużnika decyzji będzie wiązało się z wszczęciem tego postępowania. Organy administracyjne odpowiedzialne i powołane do tych czynności będą wykorzystywać wszystkie rodzaje egzekucji i będą dokładać coraz większych starań do wymuszeniu na dłużniku zobowiązania. Mowa o wymuszeniu poprzez legalne działania urzędników, by ich starania zakończyły się pozytywnym wynikiem ich postępowania.

Wiek cyfryzacji i wejście organów administracji w wirtualny świat ma pozytywny wpływ na prędkość załatwiania postępowań. Jednak często dochodzi do sytuacji, w której dłużnik nie może mimo swoich chęci spełnić świadczenia orzeczonego w decyzji np. ze względu na brak majątku lub rodzaj egzekucji – egzekucja z nieruchomości jest procesem długotrwałym. W tym miejscu należy przypomnieć raporty Najwyższej Izby Kontroli, z których wynika, że czas prowadzonych postępowań jest wydłużony. Jest to prawdopodobnie spowodowane zawiłością oraz wysokością zobowiązań wynikających z decyzji wydanych na podstawie ustawy, co wpływa na dłuższe postępowanie niż liczne postępowania sądowe prowadzone przez komorników sądowych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Paweł Gołębiewski
Akademia Ekonomiczno-Humanistyczna
w Warszawie

ROZDZIAŁ 13.

ODPOWIEDZIALNOŚĆ KARNA OSÓB DZIAŁAJĄCYCH W IMIENIU LUB NA RZECZ INSTYTUCJI OBOWIĄZANEJ

13.1. UWAGI WPROWADZAJĄCE

Współczesne wyzwania w zakresie przeciwdziałania, jak i zwalczania przestępstw związanych z praniem pieniędzy oraz finansowaniem terroryzmu nie mogą kształtować się tylko w oparciu o przepisy Kodeksu karnego, odnoszącego się do ustawowych znamion czynów zabronionych z art. 165a i art. 299 k.k. oraz penalizujących opisane w tych normach prawnych zachowania[1].

Wymienione regulacje to odpowiedź państwa na negatywne zjawiska przestępcze, jakim musi ono przeciwdziałać, i wobec tego, z uwagi na ich istotę, zostały umieszczone w Kodeksie karnym. Kodeksy zgodnie z przyjętymi regułami prawnymi, to zbiory najważniejszych aktów w polskim prawodawstwie, zawierające rozbudowane palety przepisów, regulujące dane obszary stosunków społecznych. Obowiązujący Kodeks karny z dnia 6 czerwca 1997 r.[2] wprowadzał nowe regulacje karne, które odpowiadały demokratycznemu państwu prawa, w którym prawo karne służy ochronie systemu podstawowych wartości (…), Zaś myślą przewodnią nowego prawa karnego była ochrona godności człowieka zarówno jako pokrzywdzonego, jak i sprawcy przestępstwa, a także ochrona dóbr służących człowiekowi,

[1] K. Majewski, *Zmiany w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Monitor Prawa Bankowego" 2020, nr 1, s. 92–103.

[2] Dz.U. nr 88, poz. 553.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

jego rozwojowi i pokojowemu współżyciu z innymi ludźmi[3]. Niemniej jednak, jak pokazała przyszłość, kodeks ten był wielokrotnie nowelizowany, poprzez modyfikację istniejących już regulacji prawnych lub wprowadzanie nowych artykułów penalizujących negatywne zachowania społeczne, które winny być piętnowane przez państwo. Warto jednak zwrócić uwagę, że do chwili obecnej było ponad 100 zmian w Kodeksie karnym, a mimo to nie zamieszczono w nim regulacji karnych, które pojawiły się w 2000 r. w Ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł[4]. Rozdział 8 tego nieobowiązującego już aktu prawnego, zatytułowany Przepisy karne, sankcjonował bezprawne zachowania podejmowane przez pracowników lub osoby działające w imieniu lub interesie instytucji obowiązanej. Jak więc widać, ustawodawca zauważył obszar prawa karnego wymagający interwencji i dyspozytywnego wskazania prawidłowego zachowania się przez adresata pod groźbą kary, mimo to nie zdecydował się zamieścić tego obszaru w kodeksowych regulacjach. Od 2000 r., pomimo również wielu nowelizacji aktu związanego z problematyką AML/CFT[5], w szczególności nowej odsłony tych przepisów w 2018 r.[6], nie zdecydowano się włączyć problematyki odpowiedzialności karnej osób reprezentujących instytucje obowiązane – które są zdefiniowane ustawowo – do kodeksowych regulacji karnych.

Problematyka pozakodeksowego prawa karnego w ostatnich latach zyskuje na znaczeniu. Coraz częściej wydawałoby się kluczowe zagadnienia związane z penalizacją karną znajdują się w ustawach kształtujących pod kątem formalno-prawnym określone gałęzie, sektory czy też dziedziny społecznej i administracyjno-prawnej aktywności obszarów gospodarki, jak i państwa. Rozbudowana ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, mimo iż kilkakrotnie nowelizowana, definiuje kompleksowo rolę państwa, instytucji obowiązanych i jednostek współpracujących we wspólnym wysiłku mającym na celu zwalczanie prania pieniędzy oraz finansowania terroryzmu. Zdecydowana większość przepisów w tym akcie prawnym ma charakter administracyjno-porządkowy, wskazując określone obowiązki i zasady nałożone głównie na uczestników rynku finansowego, są kluczowe w aktywnym działaniu na rzecz eliminacji przestępczych zjawisk. Takie formułowanie zapisów nie jest wyjątkiem legislacyjnym, Kodeks karny przestał być głównym zbiorem przepisów określającym czyny zabronione jako przestępstwa. Podział prawa karnego materialnego na przepisy kodeksowe oraz pozakodeksowe wskazuje, iż kryminalizacja części zachowań znajduje

[3] Wstęp do Uzasadnienia z 1995 r. do projektu Kodeksu karnego, autorzy: prof. Kazimierz Buchała i prof. Andrzej Zoll.

[4] Dz.U. z 2000 r., nr 116, poz. 1216.

[5] *Anti-Money Laundering/Counteracting Financing Terrorism* – Przeciwdziałanie praniu pieniędzy/przeciwdziałanie finansowaniu terroryzmu.

[6] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

się w ustawach, które przewidują odpowiedzialność karną uzupełniając zakres kodeksowy. Ustawy te, podobnie jak wspomniany akt z 2018 r. nie mają charakteru ściśle karnego, jest to najczęściej charakter głównie administracyjny, zaś zawarte regulacje karne mają stanowić zabezpieczenie egzekucji zawartych w nich przepisów[7]. Pozakodeksowe prawo karne w płaszczyźnie formalnej zostało podporządkowane zasadom wyrażonym w części ogólnej Kodeksu karnego. W myśl art. 116 k.k. przepisy części ogólnej kodeksu stosuje się do innych ustaw przewidujących odpowiedzialność karną, chyba że ustawy te wyraźnie wyłączają stosowanie do nich przepisów Kodeksu karnego. Wyłączenia takiego nie posiada ustawa z 2018 r., a więc przyjąć należy także w tym przypadku, iż unormowania części ogólnej Kodeksu karnego mają charakter przepisów uniwersalnych, przeznaczonych do stosowania w każdym przypadku pociągnięcia człowieka do odpowiedzialności karnej bez względu na to, w jakim miejscu usytuowano dane przestępstwo[8].

Czy jednak jest to rozwiązanie kompleksowe, pozwalające na stwierdzenie, iż system przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu jest spójny i schematyzuje współgrające ze sobą w wielu obszarach przepisy, w tym także karne pozakodeksowe, zapewniając spójną reakcję ustawodawcy na istotne naruszenia prawa.

W niniejszym rozdziale, poza odpowiedzialnością karną na podstawie przepisów AML/CFT, dokonana zostanie weryfikacja „konsekwencji ustawodawczej" wobec osób skazanych na podstawie przepisów rozdziału 14 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, koherencji z włączeniami zawartymi w przepisach prawa handlowego, dotyczącymi karalności osób, które mają zasiadać w organach spółek kapitałowych, czy też możliwości pociągnięcia do odpowiedzialności podmiotu zbiorowego, w przypadku prawomocnego skazania osoby działającej w imieniu lub w interesie podmiotu zbiorowego w ramach uprawnienia lub obowiązku do jego reprezentowania, podejmowania w jego imieniu decyzji lub wykonywania kontroli wewnętrznej albo przy przekroczeniu tego uprawnienia lub niedopełnieniu tego obowiązku[9].

13.2. MIĘDZYNARODOWE DZIAŁANIA NA RZECZ AML/CFT

Wychodząc od podwalin związanych z działaniem państwa na rzecz przeciwdziałania praniu pieniędzy, z pewnością należy przytoczyć szczyt grupy siedmiu najbar-

[7] A. Grześkowiak, K. Wiak (red.), *Prawo karne*, C.H. Beck, Warszawa 2020, s. 10.

[8] V. Konarska-Wrzosek (red.), *Kodeks karny, Komentarz*, wyd. 2, Wolters Kluwert, Warszawa 2020, s. 615.

[9] Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. z 2020 r., poz. 358, z 2021 r., poz. 1177).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

dziej wpływowych państw świata, zwanych Grupą Siedmiu lub G7, jaki odbył się dniach 19–21 czerwca 1988 r. w Toronto. Jednym z głównych tematów szczytu była walka z przestępczością narkotykową i praniem pieniędzy. Szczególną rolę w tym aspekcie odegrały Stany Zjednoczone, które w 1986 r. wprowadziły *Money Laundering Control Act*. Działania te były dalszą podstawą Stanów Zjednoczonych do podejmowania działań na rzecz poparcia wysiłków zwalczania prania pieniędzy nie tylko w zakresie krajowym, ale również na arenie międzynarodowej. Postulaty delegacji USA, choć nie spełniały wszystkich założeń związanych z powołaniem specjalnej grupy zadaniowej, zaowocowały wspólnym stanowiskiem przedstawicieli krajów uczestniczących w szczycie G7, uznającym obrót narkotykami za poważne zagrożenie. Podkreślono również konieczność podjęcia działań, które będą zmierzały do poprawy współpracy międzynarodowej w zakresie zwalczania przestępczości narkotykowej, jak i związanego z nią zjawiska prania pieniędzy.

Kolejnym krokiem w kierunków wspólnych działań na rzecz zwalczania zjawiska prania pieniędzy było powołanie przez G7, na szczycie odbywającym się w dniach 14–16 lipca 1989 r. pod Paryżem, Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (*Financial Action Task Force* – FATF)[10].

W 1990 r. przedstawiono raport na temat prania pieniędzy wraz z 40 rekomendacjami stanowiącymi inicjatywę mającą na celu walkę z tym procederem – *The Forty Recommendations of the Financial Action Task Force on Money Laundering 1990*[11].

Rekomendacje FATF zostały podzielone na cztery części:

- postanowienia ogólne,
- poprawa krajowych systemów prawnych pod kątem zwalczania prania pieniędzy oraz określenie definicji przestępstwa prania pieniędzy,
- wzrost roli systemu finansowego w przeciwdziałaniu praniu pieniędzy,
- wzmocnienie współpracy międzynarodowej w zakresie przeciwdziałania i zwalczania prania pieniędzy.

Założenia części dotyczących postanowień ogólnych wskazywały, iż każdy kraj bez zbędnej zwłoki powinien podjąć kroki w celu pełnego wdrożenia Konwencji wiedeńskiej z 1998 r.[12] i przystąpić do jej ratyfikacji. W Polsce element ten został dopełniony w 1994 r.[13]. W kolejnych założeniach podkreślano, iż tajemnice prawnie

[10] A.H. Ochnio, *Blokada rachunku i wstrzymanie transakcji jako środki przymusu w procesie karnym*, Wolters Kluwer Polska, Warszawa 2015, s. 47–55.

[11] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf (dostęp 20.9.2021 r.).

[12] Konwencja Narodów Zjednoczonych *O zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi*, sporządzona w Wiedniu dnia 20 grudnia 1988 r.

[13] Ustawa z dnia 18 lutego 1994 r. *o ratyfikacji Konwencji Narodów Zjednoczonych o zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi*, sporządzonej w Wiedniu dnia 20 grudnia 1988 r. (Dz.U. 1994 nr 43 poz. 162).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

chronione w instytucjach finansowych powinny być opracowane w taki sposób, aby nie utrudniać realizacji czterdziestu rekomendacji oraz zwrócono uwagę na poprawę wielostronnej współpracy, wzajemnej pomocy prawnej oraz ekstradycji w sprawach dotyczących prania pieniędzy.

Wzięto również pod uwagę krajowe systemy prawne pod kątem zwalczania prania pieniędzy. Rekomendacje nakazywały określenie definicji przestępstwa prania pieniędzy. Ponadto, co bardzo istotne, kraj powinien podjąć niezbędne działania, w tym legislacyjne, w celu umożliwienia kryminalizacji prania pieniędzy, w szczególności pochodzących z produkcji środków odurzających i obrotu nimi.

Wskazać należy, iż Rekomendacje FATF, zawierały sugestię kryminalizacji czynów pierwotnych będących podwalinami pod możliwość prania pieniędzy, także poza przestępstwa narkotykowe (które były niejako pierwowzorem możliwości uzyskania nielegalnych korzyści majątkowych). FATF całościowo ujmował problematykę związaną ze zjawiskiem przestępczości, wskazując wachlarz przestępczości i nielegalnych środków z niej pochodzących jako naturalnych dalszych możliwości pojawienia się zjawiska prania pieniędzy. Dlatego też kolejne rekomendacje dotyczące poprawy krajowych systemów prawnych państw odnosiły się do procesowych czynności związanych z przepadkiem korzyści majątkowych, wprowadzaniem nowych narzędzi prawnych lub rozszerzaniem istniejących, związanych z zamrażaniem i zajęciem korzyści majątkowych, także jako środki tymczasowe[14].

Rekomendacje 12–29, stanowiące trzecią część, koncentrowały się na bankach i instytucjach finansowych. Wskazywały na zasadności tworzenia i funkcjonowania systemu przeciwdziałania praniu pieniędzy w tych instytucjach. Odnosiły się do funkcjonujących obecnie narzędzi, którymi posługują się instytucje mające za zadanie podejmowanie kroków prewencyjnych w walce z tym zjawiskiem. Dotyczyły w szczególności zjawisk związanych z:

- identyfikacją klienta i zasadami przechowywania dokumentów dotyczących tych klientów,
- identyfikacją i zgłaszaniem transakcji podejrzanych,
- opracowaniem programów przeciwdziałania praniu pieniędzy,
- rejestracją wszystkich transakcji powyżej ustalonej kwoty,
- wprowadzeniem środków bezpieczeństwa finansowego,
- wykrywaniem i monitorowaniem przewozu środków pieniężnych przez granicę państw,
- wyznaczeniem organów odpowiedzialnych za prawidłowe wprowadzenie rekomendacji FATF.

[14] W. Kapica (red.), B. Paxford, R. Obczyński, M. Gawroński, W. Kapica, M. Ćwiakowski, J. Grynfelder, W. Ługowski, A. Otto, E. Patsiotos, Z. Piotrowska, J. Stolarczyk, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik*, Wolters Kluwer, Warszawa 2018.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

W czwartej części rekomendacji FATF zwrócił uwagę na wzmocnienie współpracy międzynarodowej w zakresie przeciwdziałania i zwalczania prania pieniędzy. Kraje winny podejmować działania, które umożliwią wymianę informacji dotyczących transakcji podejrzanych, w zakresie osób i podmiotów zaangażowanych w te transakcje. Międzynarodowe monitorowanie przepływów środków pieniężnych, wykorzystanie najnowszych osiągnięć przeciwdziałając i zwalczając pranie pieniędzy ma zwiększyć możliwość szacowania ilości nielegalnych środków oraz ustalenie źródła ich pochodzenia. Rekomendacje miały zwrócić uwagę krajów na korzyści płynące z wzajemnej pomocy, jak również zachęcić kraje do podpisywania wzajemnych umów i porozumień międzynarodowych, które ułatwią pomoc prawną, ekstradycję i zwiększą skuteczność w walce ze zjawiskiem prania pieniędzy.

Podkreślić należy, iż choć rekomendacje FATF nie miały charakteru prawnie wiążącego, na arenie międzynarodowej stały się istotnym wyznacznikiem stanu pożądanego i odegrały ważną rolę[15].

Powyższa problematyka zainteresowała również kraje europejskie złączone we wspólnym działaniu jako Wspólnota Europejska, a następnie Unia Europejska. Wraz z rozwojem UE opartym na trzech filarach[16]:

- filar I – espólnota Europejska (unia gospodarcza) – wspólny rynek, wspólna polityka rolna i strukturalna, unia walutowa i rozwój regionów,
- filar II – espólna polityka zagraniczna i bezpieczeństwa (unia polityczna) – UE w stosunkach zewnętrznych występuje jako jeden podmiot,
- filar III – espółpraca policyjna i sądowa w sprawach karnych (unia policyjno-sądownicza) – wspólne rozwiązywanie problemów imigracji, przestępczości zorganizowanej, terroryzmu i patologii społecznej,

pojawiła się problematyka przestępczości, w szczególności międzynarodowej. Swoboda przemieszczania się osób oraz towarów wymagała od państw członkowskich zwiększenia wspólnych wysiłków na rzecz podniesienia skuteczności współpracy na szczeblu międzynarodowym. Potrzebne było narzędzie, które zwiększyłoby potencjał wspólnych działań wskazując kierunki do ujednolicenia regulacji krajowych państw członkowskich i stowarzyszonych. Kraje były zgodne co do ryzyka, jakie pojawiło się w związku z zasadami UE związanymi w szczególności ze swobodą przemieszczania się, brakiem wewnętrznych granic oraz dostępnością do rynków państw członkowskich, które dawały większą możliwość maskowania czynności związanych z praniem pieniędzy. Nie bez znaczenia były również rekomendacje FATF z 1990 r. Dyrektywa Rady 91/308/EWG z dnia 10 czerwca 1991 r.

[15] M. Prengel, *Środki zwalczania przestępczości prania pieniędzy w ujęciu prawnoporównawczym*, TNOiK, Toruń 2003, s. 220–225.

[16] Ustanowione poprzez Traktat z Maastricht, podpisany 7 lutego 1992 r.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

w sprawie uniemożliwienia korzystania z systemu finansowego w celu prania pieniędzy[17] porządkowała wyżej wymienione kwestie. Zakładała m.in.:

- określenie definicji prania pieniędzy zgodnie z definicją przyjętą w Konwencji wiedeńskiej,
- objęcie dochodów pochodzących z każdej działalności przestępczej, nie tylko związanych z narkoprzestępczością,
- penalizację prania pieniędzy w ustawodawstwach państw członkowskich, popartą odpowiednimi środkami oraz sankcjami karnymi,
- zapewnienie, aby instytucje kredytowe i finansowe w momencie rozpoczynania świadczenia usług lub przeprowadzenia transakcji finansowych przekraczających pewne wartości progowe wymagały sprawdzenia tożsamości swoich klientów,
- przechowywanie przez instytucje kredytowe i finansowe przez okres co najmniej 5 lat kopii dokumentów tożsamości lub dokumentów dotyczących transakcji, które mogłyby być wykorzystane w postępowaniu sądowym na mocy właściwego ustawodawstwa krajowego i które mogłyby być wykorzystane jako dowody w przypadku jakiegokolwiek dochodzenia związanego z praniem pieniędzy,
- obowiązek zwracania uwagi na transakcje podejrzane, w szczególności zawierane z państwami trzecimi, które nie stosują przepisów porównywalnych z przepisami ustanowionymi przez Wspólnotę, których celem jest zapobieganie procederowi prania pieniędzy, albo innych podobnych postanowień ustalonych przez organy międzynarodowe, a które zostały uznane przez Wspólnotę,
- odnotowywanie i rejestrowanie transakcji,
- przekazywanie informacji odpowiednim organom odpowiedzialnym za przeciwdziałanie i zwalczanie prania pieniędzy,
- wprowadzenie przez instytucje kredytowe i finansowe procedur kontroli wewnętrznej oraz programów szkoleniowych.

Zgodnie z przyjętym założeniem art. 2 dyrektywy państwa członkowskie miały zapewnić, aby pranie pieniędzy w niej zdefiniowane było zabronione. Ponadto kładziono nacisk na instytucje finansowe i kredytowe, które w przyszłości w krajowych regulacjach z zakresu przeciwdziałania praniu pieniędzy zostały zdefiniowana jako instytucje obowiązane. Wymagano, by państwa członkowskie, poprzez odpowiednie narzędzia prawne:

- ustaliły odpowiednie reguły postępowania dotyczące kontroli wewnętrznej i sposobów przekazywania informacji w celu uprzedzenia i zapobiegania operacjom związanym z praniem pieniędzy,
- podjęły odpowiednie środki, mające na celu upowszechnianie wśród swoich pracowników wiedzy o przepisach zawartych w niniejszej dyrektywie.

[17] OJ L 166, 28.6.1991, p. 77–82.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Zadaniami dyrektywy było wsparcie wspólnych działań państw członkowskich na rzecz zintegrowania systemów przeciwdziałania praniu pieniędzy, poprzez przyjęcie przez nie podobnych założeń określonych w dokumencie, jak również wypełnienie idei zmniejszenia podatności rynku finansowego na wykorzystanie w celach wprowadzania środków z nielegalnych lub nieujawnionych źródeł dochodu, co miało zwiększyć stabilność krajowych systemów finansowych, a w konsekwencji również wspólnego rynku finansowego.

Regulacja ta stała się założeniem do uchwalania przez krajowego prawodawcę aktów prawnych, których zadaniem było systemowe zajęcie się problematyką prania pieniędzy. Nie wymagała ona odpowiedzialności karnej osób, które reprezentowały instytucje finansowe i kredytowe w przypadku deliktu w zakresie obowiązków wynikających ze złamania procedur związanych z przeciwdziałaniem praniu pieniędzy, ale zwracała uwagę na ich istotne znaczenie dla stabilności systemu.

13.3. KARNE REGULACJE ZA DELIKTY W USTAWIE AML/CFT

Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł[18] zapoczątkowała w polskim systemie prawnym tematykę całościowego ujęcia i skonstruowania procedur, które miały uregulować m.in. działanie instytucji finansowych i kredytowych określonych jako instytucje obowiązane, w związku ze zjawiskiem prania pieniędzy. Wprowadzała w art. 35 i art. 36 przepisy, które pod groźbą kary sankcjonowały zachowania przedstawicieli instytucji obowiązanych polegające odpowiednio na niedopełnieniu przez te osoby obowiązków określonych w ustawie czy też odmowę przekazania informacji Generalnemu Inspektorowi Informacji Finansowej lub zatajenie przed nim danych.

Jak wynika z uzasadnienia Prezesa Rady Ministrów z 26 października 1999 r., druk sejmowy III kadencji, nr 1478[19], podstawowym celem wskazanej regulacji było:

- utworzenie Generalnego Inspektora Informacji Finansowej jako organu administracji rządowej funkcjonującego przy pomocy jednostki organizacyjnej wyodrębnionej w tym celu w strukturze Ministerstwa Finansów, do którego zadań należy uzyskiwanie, gromadzenie, przetwarzanie i analizowanie informacji oraz podejmowanie działań w celu przeciwdziałania praniu pieniędzy,

[18] Dz.U. z 2000 r., nr 116, poz. 1216.

[19] https://orka.sejm.gov.pl/Rejestrd.nsf/wgdruku/1478/$file/1478.pdf, (data dostępu: 20 września 2021 r.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- wprowadzenie podziału na instytucje obowiązane, które uczestniczyły w obrocie finansowym i nałożenie obowiązków identyfikacji klienta i rejestracji określonych transakcji oraz powiadamiania o nich Generalnego Inspektora, a także zapewnienie wykonywania tych obowiązków poprzez wprowadzenie stosownych procedur kontrolnych oraz sankcji o charakterze administracyjnym (pieniężnym) bądź też karnym,
- określenie procedury wstrzymywania transakcji i blokady rachunku,
- określenie zasad ochrony i udostępniania informacji posiadanych przez Generalnego Inspektora.

Karna regulacja w powyższej ustawie nie odnosiła się do przestępstwa z art. 299 Kodeksu karnego. Przepis ten jest jedną z części systemu zwalczającego delikty w tym obszarze, ale w zakresie sprawstwa związanego z podejmowaniem czynności władczych dotyczących najogólniej mówiąc dysponowania mieniem związanym z popełnieniem czynu zabronionego. To przepisy wskazanej ustawy z 2000 r. położyły nacisk na prawidłowe wykonywanie obowiązków przez reprezentantów podmiotów obowiązanych w niej określonych. System, jaki został utworzony, zakładał już na wczesnym etapie działalności instytucji obowiązanych, możliwość karnej reakcji państwa, mającej na celu zapobieganie dalszym czynom zabronionym, narażającym cały system finansowy państwa.

Przepisy karne zawarte w art. 35–36 ogłoszonego tekstu ustawy z 2000 r. sankcjonowały zachowania osób będących pracownikami albo działającymi w imieniu lub interesie osoby prawnej lub jednostki organizacyjnej nie mającej osobowości prawnej, będącej instytucją obowiązaną, które nie dopełniły generalnie ujmując obowiązków

- niedopełnienie obowiązków związanych z rejestrację transakcji, identyfikacją klienta zgodnie z procedurami, zawiadomienia organu informacji finansowej o transakcji,
- odmawia przekazania Generalnemu Inspektorowi informacji lub dokumentów oraz przekazania danych nieprawdziwych lub zatajenie prawdziwych danych.

Była to pierwsza gruntowna reakcja ustawodawcy wychodząca naprzeciw rekomendacjom FATF oraz Dyrektywie Rady 91/308/EWG. W kolejnych latach nowelizowano akt, zmieniając również jego nazwę, która uwzględniała zachodzące w niej zmiany kierunki ewolucji. Początkowo Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu[20], zaś z dniem 22 października 2009 r. tytuł ustawy otrzymał brzmienie – Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (na podst. Dz.U. z 2009 r., nr 166, poz. 1317).

[20] Dz.U. z 2003 r., nr 153, poz. 1505.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Gruntowana zmiana aktu prawnego poświęconego tematyce AML/CFT nastąpiła w 2018 r.[21]. Wtedy m.in. doprecyzowano zadania instytucji obowiązanych, zgodnie z obowiązującym aktualnie stanem prawnym.

Aktualnie, centralnym elementem polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu jest Generalny Inspektor Informacji Finansowej (GIIF), będący sekretarzem albo podsekretarzem stanu w Ministerstwie Finansów. System przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu tworzą w Polsce:

- GIIF,
- instytucje obowiązane – podmioty zarówno z sektora finansowego, jak i niefinansowego, które oferują usługi lub produkty mogące być wykorzystane wbrew ich przeznaczeniu do prania pieniędzy lub finansowania terroryzmu, które zostały określone w art. 2 ustawy,
- jednostki współpracujące – organy administracji rządowej, organy jednostek samorządu terytorialnego oraz inne państwowe jednostki organizacyjne, a także Narodowy Bank Polski, Komisja Nadzoru Finansowego i Najwyższa Izba Kontroli.

Koncentrując się na zadaniach instytucji obowiązanych, wskazać można trzy główne kierunki związane z gromadzeniem i przekazywaniem informacji:

- dotyczące współdziałania instytucji obowiązanych z Generalnym Inspektorem Informacji Finansowej w przypadku zaistnienia uzasadnionego podejrzenia prania pieniędzy,
- inne zadania, które są związane z wypełnieniem pozostałych postanowień ustawy, w szczególności organizacyjnych[22].

Obowiązująca obecnie ustawa AML/CFT ma na celu wdrożenie w zakresie swojej regulacji m.in. IV Dyrektywę AML[23]. Zgodnie z kierunkiem działania wskazanej dyrektywy państwa członkowskie zobowiązane są do zapewnienia możliwości pociągnięcia podmiotów zobowiązanych do odpowiedzialności z tytułu naruszeń przepisów krajowych transponujących tę dyrektywę, zaś wszelkie wynikające stąd kary lub środki muszą być skuteczne, proporcjonalne i odstraszające (art. 58 dyrektywy). W wyniku zaś V Dyrektywy AML (Dyrektywa Parlamentu

[21] Ustawa z dnia 1 marca 2018 r. *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz.U. z 2018 r., poz. 723).

[22] R. Lizak, *Pranie pieniędzy w prawie polskim na tle europejskim, międzynarodowym i amerykańskim*, C.H. Beck, Warszawa 2018, s.

[23] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. *w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE*, OJ L 141, 5.6.2015, p. 73–117.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE PE/72/2017/REV/1), zobowiązano państwa członkowskie do zapewnienia, aby właściwe organy państwowe po stwierdzeniu naruszeń podlegających sankcjom karnym w odpowiednim czasie informowały o tym organy ścigania. Obszar powiadomień instytucji obowiązanych krajowych organów (GIIF), a następnie informowanie o tym organów ścigania, jest obszarem ryzyka, które trzeba wyeliminować[24].

Punkt, w którym w wyniku działania lub zaniechania działania osób znajdujących się w strukturach instytucji obowiązanej, może nie dojść do powiadomienia Generalnego Inspektora o transakcjach zawartych w ustawie z 2018 r. stanowi niejednokrotnie newralgiczny moment w możliwościach podjęcia odpowiednich i proporcjonalnych kroków przez organy państwowe, z związku z ewentualnym zjawiskiem prania pieniędzy lub finansowania terroryzmu. Ustawa dotycząca AML/CFT zawiera w rozdziale 14 zatytułowanym Przepisy karne dwa artykuły – 156 i 157, sankcjonujące:

- niedopełnienie obowiązku przekazania zawiadomień Generalnemu Inspektorowi,
- udaremnianie, utrudnianie przeprowadzenia czynności kontrolnych.

Dla porządku wskazać należy, iż czynności kontrolne i ich zakres, których udaremnianie lub utrudnianie jest karalne (art. 157), zawarto w rozdziale 12 – Kontrolowanie instytucji obowiązanych. Rozdział ten wskazuje obowiązki, jakie są stawiane instytucjom obowiązanym, m.in. w związku z koniecznością zapewnienia warunków i środków niezbędnych do sprawnego przeprowadzenia kontroli. Jednak część ta nie będzie poddawana dalszym rozważaniom.

Podkreślić należy, iż wprowadzenie aktu prawnego w 2018 r. spowodowało ograniczenie przepisów karnych w stosunku do poprzednio obowiązującego stanu prawnego. Trzeba jednak zauważyć, iż może to być spowodowane znacznym rozbudowaniem kar administracyjnych o aktualnie większym stopniu dolegliwości. Zgodnie z uzasadnieniem do ustawy, ograniczono przepisy karne ustawy przede wszystkim do penalizacji czynów, które mogą być kwalifikowane jako związane z ukrywaniem przestępnego pochodzenia środków lub zmierzające do finansowania terroryzmu, a więc do czynów odznaczających się szczególną szkodliwością[25].

Podstawową karną regulacją, jaka znajduje się w rozdziale 14, jest art. 156. Zakłada on kilka obszarów naruszeń, których może dopuścić się osoba działająca

[24] M. Dyl, M. Królikowski (red.), *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, C.H. Beck, Warszawa 2021, s. 101–108.

[25] Uzasadnienie Prezesa RM z 31 stycznia 2018 r., Druk sejmowy VIII kadencji nr 2233, k. 68.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

w imieniu lub na rzecz instytucji obowiązanej, polegających na niedopełnieniu obowiązków:

- przekazania Generalnemu Inspektorowi zawiadomienia o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu,
- obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o powzięciu uzasadnionego podejrzenia, że określona transakcja lub wartości majątkowe będące przedmiotem tej transakcji mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu.

Już na wstępie normy prawnej ustawodawca wskazuje, iż podmiot czynności w tym przypadku jest zdefiniowany, czyn zabroniony mogą popełnić konkretne osoby działające w imieniu lub na rzecz instytucji obowiązanych, a więc jest to przestępstwo indywidualne. Jak wcześniej wskazywano, system AML/CFT składa się z kilku części: GIIF, instytucji obowiązanych i jednostek współpracujących. Stabilność systemu oraz jego szczelność w przeciwdziałaniu negatywnym zjawiskom są zależne od jego uczestników i prawidłowości podejmowania przez nich czynności, do których są obowiązani, a jedynie ich spójne i harmonijne działanie zwiększa szanse na eliminację negatywnych zjawisk. Głównym przedmiotem ochrony przepisu jest więc ochrona obrotu finansowego przed wprowadzeniem do niego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł, można jednak wyróżnić uboczne przedmioty ochrony w postaci:

- prawidłowego i rzetelnego funkcjonowania instytucji obowiązanych,
- prawidłowego funkcjonowania organów administracji rządowej właściwych w sprawach przeciwdziałania praniu pieniędzy[26].

Ustawa nakłada określone obowiązki bezpośrednio na instytucje obowiązane, nie zaś na konkretne osoby. Zwrócić uwagę należy, iż przepis art. 156 działa rozszerzająco i szeroko ujmuje aktywności, jakie mogą być podejmowane w instytucjach obowiązanych. Sankcjonuje on sprzeczne z przepisami działania zarówno osób zatrudnionych w tych instytucjach – czyli pracowników, jak i osób prowadzących we własnym imieniu i na własną rzecz działalność instytucji obowiązanej. Ponadto włącza w zakres odpowiedzialności osoby działające w imieniu instytucji obowiązanych, co jednoznacznie wskazuje na zewnętrzne podmioty świadczące dla nich usługi, które mogą być na przykład agentami instytucji finansowych. Dla przyjęcia odpowiedzialności karnej wymagane jest jednak, by osoby te odpowiadały za naruszenie powierzonych im obowiązków, a nie jedynie obowiązków ustawowych instytucji obowiązanej.

[26] J. Długosz, w: *Prawo karne gospodarcze. System Prawa Handlowego*, t. 10, Warszawa 2018, s. 443.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Obowiązek przekazania GIIF zawiadomienia o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa z art. 299 k.k. – prania pieniędzy lub art. 165a k.k. finansowania terroryzmu, ciąży na instytucji obowiązanej zgodnie z art. 74 ustawy z 2018 r. Akt prawny precyzuje, iż zawiadomienie winno zostać przekazane niezwłocznie, nie później jednak niż w terminie 2 dni roboczych od dnia potwierdzenia podejrzenia przez instytucję obowiązaną. Winno ono zawierać m.in. informację oraz uzasadnienie jego przekazania[27]. Jak zauważa M. Królikowski, nastąpiła zmiana w zakresie przekazywanych informacji. Przepis przewiduje odejście od obowiązującego w poprzednim stanie prawnym mechanizmu, w którym raportowanie o podejrzeniu popełnienia przestępstwa lub finansowania terroryzmu uzależnione było od konieczności wystąpienia transakcji, której okoliczności wskazywały, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu[28]. Jeżeli instytucja obowiązana poweźmie podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, ciąży na niej obowiązek poinformowania o tym fakcie GIIF. Instytucje obowiązane mają obowiązek stosować środki bezpieczeństwa finansowego oraz analizy ryzyka, które będą stanowiły podstawy wiedzy o okolicznościach budzących wątpliwości. Zaznacza się już szerokie spektrum aktywności osoby odpowiedzialnej za poinformowanie Generalnego Inspektora o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, lub obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o powzięciu uzasadnionego podejrzenia, że określona transakcja lub wartości majątkowe będące przedmiotem tej transakcji mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu. Wszak realizacja nałożonego obowiązku musi być poprzedzona działaniem instytucji obowiązanej polegającym na podejmowaniu środków bezpieczeństwa dla właściwego wykonywania ustawowych zadań, które mogą poskutkować zawiadomieniem GIIF. Rozbudowana ustawa w rozdziale 5, zatytułowanym Środki bezpieczeństwa finansowego oraz

[27] Art. 74 ust. 3. W zawiadomieniu podaje się: 1) dane identyfikacyjne, o których mowa w art. 36 ust. 1, klienta instytucji obowiązanej przekazującej zawiadomienie; 2) posiadane dane identyfikacyjne, o których mowa w art. 36 ust. 1, osób fizycznych, osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej, niebędących klientami instytucji obowiązanej przekazującej zawiadomienie; 3) rodzaj i wielkość wartości majątkowych oraz miejsce ich przechowywania; 4) numer rachunku prowadzonego dla klienta instytucji obowiązanej przekazującej zawiadomienie, oznaczony identyfikatorem IBAN lub identyfikatorem zawierającym kod kraju oraz numer rachunku w przypadku rachunków nieoznaczonych IBAN; 5) posiadane informacje, o których mowa w art. 72 ust. 6, w odniesieniu do transakcji lub prób ich przeprowadzenia; 6) wskazanie państwa Europejskiego Obszaru Gospodarczego, z którym jest powiązana transakcja, jeżeli została przeprowadzona w ramach działalności transgranicznej; 7) posiadane informacje o rozpoznanym ryzyku prania pieniędzy lub finansowania terroryzmu oraz o czynie zabronionym, z którego mogą pochodzić wartości majątkowe; 8) uzasadnienie przekazania zawiadomienia.

[28] M. Dyl, M. Królikowski (red.), *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, C.H. Beck, Warszawa 2021, s. 23–39.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

inne obowiązki instytucji obowiązanych wskazuje katalog tych aktywności, gdzie podstawowymi są identyfikacja klienta oraz weryfikacja jego tożsamości. Procedury KYC[29] to stosowany w instytucjach finansowych podstawowy element, który wykorzystywany jest do nawiązywania stosunków gospodarczych. Z innych istotnych elementów warto jeszcze podkreślić znaczenie procedur:

- analizy transakcji przeprowadzanych w ramach stosunków gospodarczych w celu zapewnienia, że transakcje te są zgodne z wiedzą instytucji obowiązanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz zgodne z ryzykiem prania pieniędzy oraz finansowania terroryzmu związanym z tym klientem,
- badania źródła pochodzenia wartości majątkowych będących w dyspozycji klienta – w przypadkach uzasadnionych okolicznościami.

Jak słusznie wskazuje się w doktrynie, obowiązek złożenia zawiadomień, o których mowa w art. 74 ust. 1 ww. ustawy, zaktualizuje się, gdy w świadomości instytucji obowiązanej powstanie podejrzenie popełnienia przestępstwa" z art. 299 lub 165a k.k., które instytucja ta powinna być w stanie uzasadnić[30].

Przenosząc się na grunt rozważań o odpowiedzialności karnej z art. 156 ustawy wskazać należy, iż czynność sprawcza może polegać zarówno na działaniu, jak i zaniechaniu. Obejmuje on przekazanie nieprawdziwych danych czy też danych niepełnych oraz bierność instytucji obowiązanej na żądanie skierowane przez GIIF. Przepis przekazywane informacje ujmuje generalnie, tak więc dla wypełnienia jego znamion nie jest istotne, czy przekazanie nieprawdziwych lub zatajenie prawdziwych danych będą dotyczyły wszystkich informacji, dokumentów lub danych, wymaganych przepisami ustawy, czy też będzie obejmowało jedynie ich części. Czynność sprawczą niedopełnienia obowiązków można popełnić również nieumyślnie. Będzie ona polegać na niedopełnieniu określonych obowiązków w sposób niezamierzony, na przykład wynikający z niezachowania zasad ostrożności wymaganych w danych okolicznościach od osoby działającej w imieniu lub na rzecz instytucji obowiązanej. Jednak do stwierdzenia umyślności lub nieumyślności popełnienia czynu zabronionego należy posiłkować się przepisami części ogólnej Kodeksu karnego. Stwierdzenie, czy dana osoba jest sprawcą czynu umyślnego (czy nieumyślnego), wymaga jednak każdorazowego ustalenia, czy obejmowała ona świadomością, a w pewnych przypadkach i wolą, popełnienie czynu zabronionego w całym wymiarze wszystkich okoliczności tego czynu albo ustalenia ogólnego, jaki był jej stosunek psychiczny do czynu, a więc do jego

[29] *Known Your Customer.*

[30] K. Buk, *Obowiązki notariusza na podstawie przepisów ustawy z dnia 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Rejent" 2018, nr 12 (332), s. 11–29.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

poszczególnych znamion ustawowych[31]. Dlatego do przypisania odpowiedzialności sprawcy czynów z art. 156 ust. 1 pkt 1 i ust. 2[32] wystarczające będzie wykazanie, że sprawca nie zachował należytej ostrożności związanej z dopełnieniem ciążących na nim obowiązków przekazania GIIF zawiadomienia o okolicznościach wskazujących na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, zawiadomienia o transakcji lub wartości majątkowej będącej przedmiotem tej transakcji mogących mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, lub też nie zachował należytej ostrożności, której wynikiem było ujawnienie osobom nieuprawnionym informacji zgromadzonych zgodnie z komentowaną ustawą.

W przypadku każdego czynu zabronionego należy rozważyć zamiar sprawcy. Z uwagi na istotę przepisu dla stabilności systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu oraz rolę instytucji obowiązanych szczególne zabarwienie można nadać zamiarowi bezpośredniemu. Działanie przedstawiciela instytucji obowiązanej, który swoją świadomością i wolą dąży do popełnienia czynu zabronionego, niedopełnienia obowiązku przekazania zawiadomień Generalnemu Inspektorowi mogłoby spowodować zarzut popełnienia kumulatywnie być przestępstwa z art. 299 § 2 k.k.[33]. Jak wskazują jednak komentatorzy, w takim przypadku wskazana regulacja Kodeksu karnego będzie stanowiła *lex specialis w* stosunku do przepisu karnego zawartego w ustawie AML/CFT.

[31] A. Grześkowiak, K. Wiak (red.), *Kodeks karny. Komentarz*, wyd. 7, C.H. Beck, Warszawa 2021, s. 340–350.

[32] Art. 156; 1. Kto, działając w imieniu lub na rzecz instytucji obowiązanej: 1) nie dopełnia obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, lub obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o powzięciu uzasadnionego podejrzenia, że określona transakcja lub wartości majątkowe będące przedmiotem tej transakcji mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, 2) przekazuje Generalnemu Inspektorowi nieprawdziwe lub zataja prawdziwe dane dotyczące transakcji, rachunków lub osób, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

[33] Art. 299 § 2 k.k. Karze określonej w § 1 podlega, kto będąc pracownikiem lub działając w imieniu lub na rzecz banku, instytucji finansowej lub kredytowej lub innego podmiotu, na którym na podstawie przepisów prawa ciąży obowiązek rejestracji transakcji i osób dokonujących transakcji, przyjmuje, wbrew przepisom, środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, dokonuje ich transferu lub konwersji, lub przyjmuje je w innych okolicznościach wzbudzających uzasadnione podejrzenie, że stanowią one przedmiot czynu określonego w § 1, lub świadczy inne usługi mające ukryć ich przestępne pochodzenie lub usługi w zabezpieczeniu przed zajęciem.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

13.4. SKAZANIE NA PODSTAWIE USTAWY AML/CFT A PIASTOWANIE FUNKCJI LUB STANOWISKA W PODMIOTACH GOSPODARCZYCH

Jak wskazano powyżej, również ustawa z 2018 r., mimo iż w większość zawiera przepisy administracyjno-porządkujące, zawiera regulacje karne i nie jest to nic nietypowego dla polskiego systemu prawnego. Pozakodeksowe przepisy karne, dbają o kształtowanie prawidłowego sposobu postępowania i możliwości egzekwowania i rugowania deliktów przestępczych. System przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu wpisuje się w wiele obszarów prawa. Korzysta z zasad prawa cywilnego, administracyjnego, jak i polega w zdecydowanej mierze na spójności sektora finansowego[34], który stanowi trzon systemu jako instytucje obowiązane współpracujące z Generalnym Inspektorem Informacji Finansowej.

Prawo karne, mimo iż zostało podzielone na kodeksowe i pozakodeksowe, nie bacząc na doniosłość aktu prawnego, w którym zostały zawarte konkretne regulacje, winno być spójne i dążyć do jednego wspólnego celu, jakim są narzędzia w rękach ustawodawcy, mające na celu eliminowanie patologicznych zachowań. System więc tworzą w tym momencie różne przepisy karne wzajemnie ze sobą współpracujące i chroniące określone dobra. Regulacja z art. 156 Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, również powinna wpisywać się w szeroki plan twórców aktów prawnych, tworząc wzajemnie spójne i uzupełniające się normy, wyraźnie eliminujące „słabe ogniwa" mogące zagrozić stabilności systemu AML/CFT. Czy jednak tak się dzieje?

Wymienione we wskazanym powyżej przepisie obowiązki to niejednokrotnie w mniejszych podmiotach gospodarczych zadania członków zarządów, którzy pełnią jednocześnie formalnie lub nieformalnie rolę oficerów AML, zaś ich zadaniem jest współpraca z GIIF w zakresie obowiązku zawiadomienia o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, lub obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o powzięciu uzasadnionego podejrzenia, że określona transakcja lub wartości majątkowe będące przedmiotem tej transakcji mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, przekazując informacje pełne i prawdziwe.

[34] P. Sitek, *Wpływ skali i struktury finansowania, sektora przedsiębiorstw, na gospodarkę…* (w:) *Sytuacja prawno-finansowa przedsiębiorców sektora małych i średnich przedsiębiorstw*, red. A. Niemczyk-Wójcik, T. Talar, Warszawa 2016, s. 181–196.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Celem uniemożliwienia wykorzystywania spółek kapitałowych przez osoby które mają kryminalną przeszłość Kodeks spółek handlowych wprowadził regulację warunków pełnienia funkcji. Zgodnie z aktualnym brzmieniem art. 18 k.s.h.:

- § 1. Członkiem zarządu, rady nadzorczej, komisji rewizyjnej albo likwidatorem może być tylko osoba fizyczna mająca pełną zdolność do czynności prawnych.
- § 2. Nie może być członkiem zarządu, rady nadzorczej, komisji rewizyjnej, likwidatorem albo prokurentem osoba, która została skazana prawomocnym wyrokiem za przestępstwa określone w przepisach rozdziałów XXXIII–XXXVII Kodeksu karnego oraz w art. 585, art. 587, art. 590 i art. 591 ustawy.
- § 3. Zakaz, o którym mowa w § 2, ustaje z upływem piątego roku od dnia uprawomocnienia się wyroku skazującego, chyba że wcześniej nastąpiło zatarcie skazania.
- § 4. W terminie trzech miesięcy od dnia uprawomocnienia się wyroku, o którym mowa w § 2, skazany może złożyć wniosek do sądu, który wydał wyrok, o zwolnienie go z zakazu pełnienia funkcji w spółce handlowej lub o skrócenie czasu obowiązywania zakazu. Nie dotyczy to przestępstw popełnionych umyślnie. Sąd rozstrzyga o wniosku, wydając postanowienie.
- § 5. Przepisy § 1–4 stosuje się do członka zarządu spółki partnerskiej oraz członka rady nadzorczej spółki komandytowo-akcyjnej[35].

Kluczowy w tej normie prawnej paragraf drugi w tekście ogłoszonym w 2000 r., zawierał nieco inne postanowienia:

- § 2. Nie może być członkiem zarządu, rady nadzorczej, komisji rewizyjnej albo likwidatorem osoba, która została skazana prawomocnym wyrokiem za przestępstwa określone w przepisach rozdziałów XXXIII–XXXVII Kodeksu karnego oraz w art. 585, art. 587, art. 590 i w art. 591 ustawy[36].

Jak więc widać, przez ponad dwie dekady obowiązywania kodeksu ustawodawca zdecydował się rozszerzyć katalog osób, które podlegają w spółce kapitałowej szczególnemu rygorowi o prokurenta. Zważywszy na istotne znaczenie prokury jako szczególnego rodzaju pełnomocnictwa udzielanego przez przedsiębiorcę podlegającego obowiązkowi wpisu do rejestru przedsiębiorców, nie jest to zmiana zaskakująca. Pełnomocnictwo to pozwala na dokonywanie wszelkich czynności sądowych i pozasądowych, jakie związane są z prowadzeniem przedsiębiorstwa w granicach jego umocowania, wywołując skutki prawne dla przedsiębiorcy, wobec czego istotne jest, by była to osoba o ugruntowanej opinii.

Utworzony w art. 18 k.s.h. katalog czynów zabronionych eliminuje z mocy ustawy w przypadku skazania, z możliwości bycia członkiem zarządu, rady nadzorczej, komisji rewizyjnej, likwidatorem albo prokurentem spółki kapitałowej,

[35] Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych, t.j. Dz.U. z 2020 r. poz. 1526.
[36] Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych, Dz.U. 2000 nr 94, poz. 1037.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

pomija czyn zabroniony istotny dla stabilności systemu finansowego, wynikający z ustawy AML/CFT.

Aktualnie regulacje Kodeksu spółek handlowych wskazują na negatywną przesłankę wynikającą ze skazania za popełnienie następujących deliktów karnych:

- przestępstwa przeciwko ochronie informacji, art. 265–269 k.k. (np. bezprawne uzyskanie),
- przestępstwa przeciwko wiarygodności dokumentów, art. 270–277 k.k. (np. fałszowanie podpisu, poświadczenie nieprawdy, posługiwanie się czyimś dokumentem),
- przestępstwa przeciwko mieniu, art. 278–295 k.k. (np. kradzież, kradzież z włamaniem, rozbój, przywłaszczenie, oszustwo, zniszczenie mienia),
- przestępstwa przeciwko obrotowi gospodarczemu, art. 296–309 k.k. (np. wyrządzenie szkody w obrocie, łapownictwo na stanowisku kierowniczym, wyłudzenie odszkodowania, pranie brudnych pieniędzy, pokrzywdzenie wierzyciela),
- przestępstwa przeciwko obrotowi pieniędzmi i papierami wartościowymi, art. 310–316 k.k. (np. fałszowanie pieniędzy i puszczanie ich w obieg),
- ujawnianie fałszywych danych związanych z działalnością gospodarczą (art. 587 k.s.h.),
- umożliwienie bezprawnego głosowania (art. 590 k.s.h.),
- udział w bezprawnym głosowaniu (art. 591 k.s.h.).

Dla porządku wskazać należy, iż w wyniku zmian przepisów wprowadzonych Ustawą z dnia 9 czerwca 2011 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. nr 133, poz. 767), która weszła w życie 13 lipca 2011 r. uchylony został art. 585 k.s.h., który regulował odpowiedzialność karną osób działających na szkodę spółki handlowej, a którego zdaniem wielu komentatorów, przedmiot ochrony pozostał zbieżny z art. 296 k.k.

Artykuł 18 § 2 i 3 k.s.h. wskazuje katalog przestępstw, których popełnienie skutkuje zakazem uczestnictwa w organach spółki kapitałowej. Zakaz ten powstaje *ex lege* z chwilą uprawomocnienia się wyroku skazującego za przestępstwa określone w komentowanym przepisie i trwa przez okres 5 lat od dnia uprawomocnienia się wyroku, chyba że wcześniej nastąpiło zatarcie skazania[37]. Niemożność pełnienia funkcji powoduje, iż osoba taka nigdy nie zyska statusu członka zarządu, rady nadzorczej, komisji rewizyjnej, likwidatora albo prokurenta. W przypadku jednak uchwały powołującej taką osobę na wskazane funkcje, jej ewentualne działania przedsięwzięte w ramach tych funkcji w żadnym razie nie będą traktowane

[37] J. Bieniak, M. Bieniak, G. Nita-Jagielski, *Kodeks spółek handlowych. Komentarz*, wyd. 7, C.H. Beck, Warszawa 2020, s. 135–140.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

w kategorii doniosłego działania członka zarządu, rady nadzorczej, komisji rewizyjnej, likwidatora albo prokurenta[38].

Dla podkreślenia znaczenia tego przepisu w odniesieniu do ochrony obrotu gospodarczego, a więc ewentualnego wpływu na system gospodarczy, gdzie państwo jako regulator winno stworzyć właściwe i przejrzyste procedury sprzyjające rozwojowi oraz zabezpieczające przed negatywnymi działaniami, warto przytoczyć kilka orzeczeń zwracających uwagę na znaczenie tego unormowania.

Zgodnie z postanowieniem Sądu Apelacyjnego w Krakowie prawomocne skazanie za przestępstwo wymienione w art. 18 § 2 k.s.h. sprawia, że osoba zainteresowana piastowaniem funkcji określonych w tym przepisie nie posiada zdolności do ich pełnienia. Skutki te wynikają ex lege z wydania prawomocnego wyroku skazującego, nie można ich więc utożsamiać ze stosowaniem zakazu pełnienia funkcji jako środka o charakterze penalnym[39]. Rozważyć wobec tego można, znaczenie przepisu. Praktyka pokazywała niejednokrotnie, iż osoby, w stosunku do których pojawiła się wskazana negatywna przesłana skazania, pełniły dalej funkcje, które od momentu prawomocnego skazania za określone czyny są dla nich niedostępne. Czy wobec braku zdolności do pełnienia funkcji osoba powołana na przykład przy działaniu mocodawców w błędzie uwalnia się od odpowiedzialności za podjęte działania w przedsiębiorstwie, czy też można pociągnąć ją do odpowiedzialności, mimo iż zaistniała negatywna przesłanka. Problematyka ta może być szczególnie widoczna na przykładzie zobowiązań względem wierzycieli, jak i zaległości względem organów skarbowych. Jak wskazuje orzecznictwo: osoba, która faktycznie pełniła funkcję członka zarządu w okresie, w którym powstały zobowiązania podatkowe, nie może powoływać się na okoliczność, że nie mogła pełnić tej funkcji z uwagi na zakaz wynikający z art. 18 § 2 k.s.h., dla uwolnienia się od odpowiedzialności za zaległości podatkowe, którą ponosi na podstawie art. 116 Ordynacji podatkowej[40].

Przepis z art. 18 k.s.h. ma więc charakter uniwersalny. Chroni obrót gospodarczy, nie wyłączając jednak od ewentualnej odpowiedzialności działania osoby, które mimo zaistnienia okoliczności negatywnych – skazania na podstawie wymienionych regulacji – dalej podejmowały działania, w tym niekorzystne dla przedsiębiorstwa,

Zwrócić należy uwagę na zabieg legislacyjny ustawodawcy, który w art. 18 k.s.h. wymienił całe rozdziały z Kodeksu karnego, a także nieliczne przepisy karne z Kodeksu spółek handlowych. Łączność pomiędzy prawem spółek a prawem karnym, podobnie jak i w niektórych obszarach przepisów zwalczają-

[38] Z. Jara (red.), *Kodeks spółek handlowych. Komentarz*, wyd. 3, C.H. Beck, Warszawa 2020, s. 150–152.

[39] Postanowienie Sądu Apelacyjnego w Krakowie – II Wydział Karny z dnia 9 listopada 2017 r. II AKz 414/17.

[40] Wyrok Naczelnego Sądu Administracyjnego z dnia 3 grudnia 2020 r. II FSK 2185/18.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

cych pranie pieniędzy oraz finansowanie terroryzmu, związana jest z działalnością gospodarczą. Jak wskazano w uzasadnieniu projektu ustawy wprowadzającej Kodeksu karnego w 1997 r., w szczególności odnoszącej się do rozdziału przestępstw gospodarczych, rozwiązania ukierunkowane na gospodarkę wolnorynkową mają za zadanie ochronę reguł obrotu gospodarczego gospodarki wolnorynkowej z możliwym interwencjonizmem państwa, skierowane zwłaszcza przeciwko wynaturzeniom, przynoszącym szkodę podmiotom uczestniczącym w działalności gospodarczej lub też państwu[41]. Czy taka intencja prześwietla obecnie ustawodawcy, który nie rozszerza katalogu wyłączeń zawartych w art. 18 k.s.h. Wszak nie sposób nie zauważyć, iż przepisy głównego źródła odpowiedzialności karnej za przestępstwa w obrocie gospodarczym, a więc Rozdziału XXXVI Kodeksu karnego – „Przestępstwa przeciwko obrotowi gospodarczemu", były już nowelizowane kilkanaście razy. Ponadto, jak słusznie wylicza R. Zawłocki[42], odpowiedzialność karna za pozakodeksowe przestępstwa gospodarcze wskazana jest w niemal 60 ustawach z zakresu obrotu gospodarczego i obejmuje łącznie blisko 300 przestępstw typu podstawowego (z wyróżnieniem przestępstw umyślnych i nieumyślnych). Analizując akty prawne dotyczące obrotu gospodarczego, wskazać można na rosnącą liczbę pozakodeksowych regulacji karnych.

Rosnące znaczenie narzędzi AML/CFT już na wczesnym etapie winno nie dopuszczać do zaistnienia ryzyka wykorzystania leganie funkcjonujących podmiotów do czynności przestępczych, a tym samym ułatwiać omijanie tworzonego od lat systemu. Pranie pieniędzy jest procesem złożonym i trudno mówić tu o jednym przyjętym schemacie, raczej winniśmy mówić o trendach, które są wypadkową wielu elementów: rodzaju przestępczości (kryminalne, gospodarcze), rodzaju nielegalnego aktywa, jak również uwarunkowań prawnych, a w szczególności możliwych do wykorzystania luk, które spowodują, iż system na wczesnym, można by powiedzieć prewencyjnym, etapie nie ostrzeże o potencjalnym zagrożeniu. Przyjęło się, iż wprowadzanie dochodów z niedozwolonych i nieujawnionych źródeł do finansowego ekosystemu oraz ich obieg, a także wyprowadzanie tych środków do legalnego obrotu gospodarczego odbywa się zazwyczaj w trzech etapach: lokowanie, maskowanie, integrowanie, które mogą wystąpił łącznie, osobno, jak również mogą się przenikać. Nadrzędnym celem tych aktywności jest ukrycie ich związku z przestępczymi działaniami, a wobec tego w każdej z faz pomocnym elementem, anonimizującym w pewnym stopniu, może być spółka kapitałowa.

Przepis karny z art. 156 AML/CFT dotyczy zarówno działania, jak i zaniechania sprawcy. Co także istotne, niedopełnienie obowiązku przekazania informacji, o którym mowa ww. normie prawnej, oraz ujawnienie osobom nieupraw-

[41] Uzasadnienie, rozdz. XXXVI, pkt 1.

[42] *Prawo Karne Gospodarcze, System Prawa Handlowego,* red. R. Zawłocki, t. 10, wyd. 2, C.H. Beck, Warszawa 2018, s. 345–350.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

nionym, posiadaczom rachunku lub osobom, których transakcja dotyczy, informacji zgromadzonych zgodnie z komentowaną ustawą lub wykorzystanie tych informacji, o którym mowa w ustępie drugim, może zostać dokonane zarówno umyślnie, jak i nieumyślnie. Wobec szerokiego frontu budowania systemu AML/CFT trudno oprzeć się wrażeniu, iż w zakresie eliminowania uczestników rynku, którzy mogą zajmować się prowadzeniem faz prania pieniędzy, regulacja ta winna zostać uwzględniona w art. 18 k.s.h. Zdając sobie sprawę z obowiązków nałożonych na reprezentantów spółek kapitałowych, dla przejrzystości gospodarki istotne znaczenie mają kwalifikacje osób zarządzających podmiotami i ich przeszłość, także kryminalna, by ewentualne negatywne skutki działań podmiotu nie mogły wywrzeć negatywnego skutku dla innych uczestników rynku. Zarządzanie spółką przez osobę, która w przeszłości ignorowała normy zobowiązujące do współpracy z Generalnym Inspektorem Informacji Finansowej, a z pewnością, która robiła to umyślnie, winno być również rozpatrywane przez pryzmat dawania przez nią rękojmi właściwego wykonywania obowiązków czy choćby prewencyjne działanie, niedopuszczające do tworzenia i zarządzanie przez nią kolejnymi nowymi podmiotami, które mogą być elementem maskowania.

Dla porównania, można przywołać *lex specialis* w stosunku do Kodeksu spółek handlowych i zawartą regulację z art. 18, a mianowicie Prawo bankowe. Banki stanowią największą grupę instytucji obowiązanych wymienionych w akcie pranym dotyczącym przeciwdziałaniu prania pieniędzy oraz finansowaniu terroryzmu. Z uwagi na charakter ich działalności ustawodawca w sposób szczególny przykłada uwagę do osób piastujących w nich funkcje oraz wprowadza liczne wymagania wobec kandydatów do pełnienia funkcji członków zarządu banku[43]. Zgodnie z art. 22b Ustawy z dnia z dnia 29 sierpnia 1997 r. Prawo bankowe t.j. Dz.U. z 2020 r. poz. 1896, Komisja Nadzoru Finansowego wyraża zgodę na powołanie na członka zarządu osoby, na wniosek rady nadzorczej, która wraz z wnioskiem o wyrażenie zgody, przekazuje informacje i oświadczenia osób ubiegających się o to stanowisko, w tym, odnoszące się do okresu ostatnich 5 lat, dotyczące m.in. karalności tych osób, prowadzonych przeciwko nim postępowań karnych i postępowań w sprawach o przestępstwa skarbowe[44]. Ustawodawca w tym zakresie wskazuje na konieczność weryfikacji przesłanki rękojmi, jaką musi spełniać kandydat.

Takie ujęcie wskazanej problematyki powoduje, iż osoba skazana na podstawie art. 156 ustawy AML/CFT w przypadku umyślności działania automatycznie nie spełniałaby kryteriów pozwalających na zajęcie funkcji w instytucji obowiązanej. Należy zwrócić jeszcze uwagę na fakt, iż czyn niedopełnienia obowiązku prze-

[43] P. Gołębiewski, *Bank jako instytucja zaufania publicznego (rozdział V), Prawne gwarancje bezpieczeństwa bankowego (rozdział VI), Nadzór nad stabilnością systemu bankowego (rozdział VII)* (w:) *Prawo bezpieczeństwa finansowego. Wybrana problematyka*, red. M. Karpiuk, M. Sawicka, P. Sitek, Olsztyn 2016, s. 179–223.

[44] Art. 22b ust 2 pkt 4 Ustawy z dnia z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. z 2020 r. poz. 1896).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

kazania zawiadomień Generalnemu Inspektorowi, jak wynika z Ustawy z dnia 1 kwietnia 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, można również popełnić nieumyślnie. Jednak w przypadku Ustawy Prawo bankowe ustawodawca przewidział dodatkowe możliwości władczej decyzji organu sprawującego m.in. nadzór nad sektorem bankowym[45], przyznając KNF możliwości odmowy wyrażenia zgody na powołanie członków zarządu, jeżeli:

- jest prowadzone przeciwko nim postępowanie karne lub postępowanie w sprawie o przestępstwo skarbowe,
- były karane za przestępstwo inne niż przestępstwo umyślne lub przestępstwo skarbowe, z wyłączeniem przestępstw ściganych z oskarżenia prywatnego.

W takim przypadku, bacząc na normy karne zawarte ustawie AML/CFT, Komisja Nadzoru Finansowego mogłaby nawet w okolicznościach nieumyślności działania kandydata na członka zarządu dokonać jego weryfikacji. Popełniony przez kandydata w przeszłości delikt braku współpracy z Generalnym Inspektorem w typie uprzywilejowanym, skutkowałby możliwością odmowy wyrażenia zgody na powołanie go na członka zarządu.

Wskazać należy, iż regulacje zawarte w art. 22b Ustawy Prawo bankowe znajdują odpowiednie stosowanie w przypadku banku spółdzielczego[46]. Zgodnie z art. 18 Ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych[47] członkami rady nadzorczej i zarządu kasy mogą być wyłącznie osoby, które nie były prawomocnie **skazane** za przestępstwo umyślne przeciwko mieniu, dokumentom lub przestępstwo skarbowe. Rozwiązania przyjęte w tym akcie prawnym również zakładają udział Komisji Nadzoru Finansowego w akceptacji procesu wyłaniania prezesa zarządu kasy, gdzie podobnie jak w prawie bankowym KNF odmówi wyrażenia zgody w przypadku, gdy kandydat był karany za przestępstwa umyślne, zaś może odmówić – a więc poddane jest pod rozwagę organu nadzorczego – w przypadku skazania za przestępstwo nieumyślne.

Procedura taka obowiązuje jedynie w przypadku prezesa zarządu kasy, jak więc wynika z przepisów ustawy, członkiem zarządu kasy (z wyłączeniem jej prezesa), może zostać osoba skazana za przestępstwo nieumyślnie, a więc ponownie wchodzi w zakresu typu uprzywilejowanego art. 156 ustawy AML/CFT.

Czy wobec tego w kontekście przestępstwa prania pieniędzy lub finansowania terroryzmu możliwość powołania na członka zarządu kasy osoby karanej za typ uprzywilejowany przestępstwa niedopełnienia obowiązku przekazania zawiado-

[45] P. Gołębiewski, *Ramy prawne blokady rachunku bankowego i wstrzymania transakcji płatniczej* (w:) *Pieniądz i jego oddziaływanie na otoczenie*, red. P. Sitek, recenzowana praca zbiorowa, Warszawa 2016, s. 155–193.

[46] Art. 20a Ustawy z dnia z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. z 2020 r., poz. 1896).

[47] T.j. Dz.U. z 2020 r., poz. 1643.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

mień Generalnemu Inspektorowi jest celowym zabiegiem, czy też omyłkowym pominięciem ustawodawcy.

Skoro ustawodawca nie zamieszcza w prewencyjnej możliwości przeciwdziałania zakazów powoływania osób skazanych do istotnych w spółkach kapitałowych organów, czy wobec tego zakłada możliwość odpowiedzialności spółki jako podmiotu zbiorowego, w przypadku popełnienia deliktu karnego związanego z ustawą AML/CFT? Mogłoby to być wszak działaniem wymuszającym w odniesieniu do samego podmiotu, który bacząc na możliwość swojej odpowiedzialności, która połączona może być z różnego rodzaju dolegliwościami finansowymi, obejmowałby specjalnym nadzorem decyzyjne osoby w firmie, na przykład przez tworzenie procedur kontrolno-nadzoryczych. Czy w ogóle taka odpowiedzialność jest możliwa?

Do polskiego systemu prawnego taką odpowiedzialność wprowadziła ustawa z 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz.U. z 2020 r. poz. 358), jako przestępstwa lub przestępstwa skarbowe oraz zasady postępowania w przedmiocie takiej odpowiedzialności. Zgodnie z art. 2 ust. 1 obowiązująca od 28 października 2003 r. ustawy, podmiotem zbiorowym jest osoba prawna oraz jednostka organizacyjna niemająca osobowości prawnej, której odrębne przepisy przyznają zdolność prawną, z wyłączeniem Skarbu Państwa, jednostek samorządu terytorialnego i ich związków. Artykuł 2 ust. 2 wskazanej ustawy precyzuje, że podmiotem zbiorowym w rozumieniu ustawy jest również spółka handlowa z udziałem Skarbu Państwa, jednostki samorządu terytorialnego lub związku takich jednostek, spółka kapitałowa w organizacji, podmiot w stanie likwidacji oraz przedsiębiorca niebędący osobą fizyczną, a także zagraniczna jednostka organizacyjna[48].

Podmiot zbiorowy podlega odpowiedzialności za czyn zabroniony, którym jest zachowanie osoby fizycznej:

1) działającej w imieniu lub w interesie podmiotu zbiorowego w ramach uprawnienia lub obowiązku do jego reprezentowania, podejmowania w jego imieniu decyzji lub wykonywania kontroli wewnętrznej albo przy przekroczeniu tego uprawnienia lub niedopełnieniu tego obowiązku,

2) dopuszczonej do działania w wyniku przekroczenia uprawnień lub niedopełnienia obowiązków przez osobę, o której mowa w pkt 1,

3) działającej w imieniu lub w interesie podmiotu zbiorowego, za zgodą lub wiedzą osoby, o której mowa w pkt 1,

3a) będącej przedsiębiorcą, który bezpośrednio współdziała z podmiotem zbiorowym w realizacji celu prawnie dopuszczalnego,

4) (uchylony)

[48] *Pokrzywdzony jako uczestnik postępowań represyjnych. Czwarty wierzchołek trójkąta?*, red. P. Czarnecki, C.H. Beck, Warszawa 2021, s. 240–250.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

– jeżeli zachowanie to przyniosło lub mogło przynieść podmiotowi zbiorowemu korzyść, chociażby niemajątkową[49].

Stosownie do art. 16 ust. 1 pkt. 1 lit. a) tej ustawy, podmiot zbiorowy podlega odpowiedzialności karnej m.in. za pranie pieniędzy, jeżeli dopuści się go osoba fizyczna, o której mowa w art. 3 tej ustawy[50]. Dotyczy to wprost czynności sankcjonowanej Kodeksem karnym. Katalog zbudowany w ustawie o odpowiedzialności podmiotów zbiorowych zawiera, ponownie jak w przypadku art. 18 k.s.h., enumeratywnie wskazane normy prawne, z wielu aktów prawnych związanych m.in. z obrotem gospodarczym, ale i ochroną środowiska, czy też ochroną zdrowia. Ponownie jednak brakuje tam uregulowań karnych wymienionych w ustawie AML/CFT. Czy brak współpracy z Generalnym Inspektorem, mógłby przynieść pomiotowi korzyść, która jest jednym z niezbędnych warunków odpowiedzialności, na podstawie tej ustawy?

Nietrudno sobie wyobrazić przesłanki, które mogłyby kierować osobą zajmującą się przestępczym procederem dopuszczającą się zaniedbania obowiązków zawiadamiania GIIF o transakcjach podejrzanych, a przecież zgodnie z ustawą AML/CFT są to choćby transakcje gotówkowe (powyżej 10 000 EUR). Cała gama posunięć, w postaci transakcji, które przyniosą podmiotowi zbiorowemu różnego rodzaju benefity, czy to w postaci prowizji, czy też zwiększonej ilości zamówień z uwagi na działanie w „szarej strefie", które może być pożądane w niektórych kręgach, może wiązać się dla niego z korzyścią majątkową. Można wszak będzie powiązać te zaniechania (w szczególności celowe) z wystąpieniem przeciwko obowiązkom wynikającym ustawy AML/CFT. Dlaczego wobec tego ustawodawca pomija te działania? Na marginesie tylko wypada podać, iż w projektowanej nowelizacji ustawy o odpowiedzialności podmiotów zbiorowych za czyny popełnione pod groźbą kary, która od kilku lat czeka w opracowaniach sejmowych[51], ustawodawca zakłada, iż każdy delikt karny osoby generalnie ujmując podejmującej decyzje w podmiocie zbiorowym, może powodować odpowiedzialność tego podmiotu, tak więc będzie to katalog otwarty. Jednak zgodnie z obecnym stanem prawnym, regulacje karne z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu nie wchodzą w zakres ew. dalszej penalizacji podmiotu zbiorowego w przypadku wypełnienia przesłanek ustawowych.

Czy wobec tego ustawodawca celowo różnicuje poziomy instytucji obowiązanych wymienionych katalogu zawartym w artykule drugim ustawy z 1 marca 2018 r. o przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu? Jak

[49] Art. 3 Ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. Dz.U. z 2020 r., poz. 358).

[50] A. Golonka, *Polskie regulacje karne wobec „szóstej" dyrektywy Anti-Money Laundering*, „IUSNOVUM" 2021, nr 1, s. 29.

[51] https://legislacja.rcl.gov.pl/projekt/12312062 (data dostępu: 21.09.2021 r.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wskazuje przyjęta tam kolejność zarówno banki, jak i spółdzielcze kasy oszczędnościowo-kredytowe są wymienione jako pierwsze, zaś przedsiębiorcy funkcjonujący w myśl Ustawy z dnia z dnia 6 marca 2018 r. Prawo przedsiębiorców (Dz.U. z 2021 r., poz. 162), także zgodnie z Kodeksem spółek handlowych, znajdują się w dalszej kolejności, rozszerzanej nowelizacjami listy.

Generalnymi celami, jakim mają podlegać uczestnicy systemu AML, jest m.in.:

- zapobieganie jego wykorzystaniu do prania pieniędzy i finansowania terroryzmu,
- zapewnienie integralności, stabilności i wiarygodności sektora finansowego,
- zwiększenie transparentności przepływów finansowych,
- doprecyzowanie zakresu stosowania przez instytucje obowiązane środków bezpieczeństwa finansowego.

Podkreślić należy w ślad za twierdzeniami dyrektywy, iż integralność unijnego systemu finansowego zależy od przejrzystości podmiotów o charakterze korporacyjnym oraz innych podmiotów prawnych, trustów i podobnych porozumień prawnych. Niniejsza dyrektywa ma na celu nie tylko wykrywanie przypadków prania pieniędzy i prowadzenie dochodzeń w ich sprawie, ale także zapobieganie ich wystąpieniu. Zwiększanie przejrzystości mogłoby być skutecznym środkiem odstraszającym[52]. Uniemożliwienie wprowadzania do legalnego obrotu finansowego środków i wartości majątkowych pochodzących z działalności przestępczej – czyli nielegalnych źródeł czy też nieujawnionych – a więc takich, które związane są z szarą strefą, powiązaną jednocześnie z unikaniem opodatkowania, wymaga zwrócenia uwagi na osoby zarządzające podmiotami gospodarczymi.

Rola podmiotów gospodarczych z pewnością zostaje przez ustawodawcę dostrzeżona w kolejnych nowelizacjach ustawy AML/CFT. Tylko w bieżącym roku, kolejne nowelizacje powodują:

- rozszerzenie katalogu instytucji obowiązanych poprzez dołączenie do nich:
  - pośredników w obrocie nieruchomościami,
  - przedsiębiorców, których podstawową działalnością gospodarczą jest świadczenie usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego,
  - przedsiębiorców zajmujących się obrotem lub pośrednictwem w obrocie dzieł sztuki i antyków,
- zmiany w zakresie weryfikacji beneficjenta rzeczywistego:
  - weryfikacja beneficjenta rzeczywistego nie może polegać wyłącznie na weryfikacji w CRBR (Centralny Rejestr Beneficjentów Rzeczywistych),
  - rozszerzono katalog podmiotów, które muszą zgłaszać beneficjenta rzeczywistego o CRBR,

[52] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

  - nałożono obowiązki dostarczania informacji instytucjom obowiązanym wprost na beneficjentów rzeczywistych,
- obowiązek wpisu do rejestru dla niektórych instytucji obowiązanych:
  - przedsiębiorcy prowadzący działalność na rzecz spółek lub trustów oraz działalność w zakresie walut wirtualnych będą podlegali wpisowi do odpowiednich rejestrów, zaś uzyskanie wpisu jest warunkiem możliwości świadczenia powyższych usług.

Zmieniająca się sytuacja gospodarcza związana z rozwojem technologii powoduje, iż niejednokrotnie ustawodawca nie jest jednak w stanie doprecyzować w normach prawnych wszelkiej aktywności gospodarczej, która może być podatna na zagrożenia związanie z praniem pieniędzy oraz finansowaniem terroryzmu. Konieczność uszczelnienia systemu AML/CFT, zazwyczaj związana jest z pojawianiem się nowych trendów w sektorze finansowym. Najbardziej efektownym przykładem, który będzie obrazował problematykę jest w tej chwili technologia blockchain wykorzystywana w cyfrowych walutach. Podmioty zajmujące się różnego rodzaju aktywnością w tym zakresie mogą być typowymi spółkami prawa handlowego lub nawet działalnościami gospodarczymi. W takim przypadku rodzi się pytanie, czy w parze ze zmianami pojawiającymi się w ustawie o przeciwdziałaniu praniu pieniędzy, ustawodawca nie powinien rozszerzyć katalog zawarty w art. 18 k.s.h., poprzez większą paletę deliktów stanowiących negatywną przesłankę do zajmowania określonej funkcji czy stanowiska.

Błędem byłoby myślenie, iż taka zmiana samoistnie rozwiąże wątpliwości jakie mogą się pojawić na gruncie systemu AML/CFT. Jeżeli jednak osoba skazana za przestępstwa związane z brakiem współpracy z Generalnym Inspektorem wymaganej ustawą, zarówno z typie podstawowym jak i uprzywilejowanym, może zostać na przykład członkiem zarządu spółki, która następnie będzie instytucją obowiązaną, wymaga to postawienia pytania, czy jest to dobre rozwiązanie prawne.

13.5. DZIAŁANIA KONTROLNE GENERALNEGO INSPEKTORA

Generalny Inspektor Informacji Finansowanej co roku w swoich raportach z działalności podaje statystyki związane z czynności kontrolnych jakie wykonał. Z uwagi na omawianą nowelizację ustawy w 2018 r., zasadnym jest dokonać porównania wyników z lat 2019 i 2020, więc lat, gdy ustawa obowiązywała w pełnym roku kalendarzowym.

W 2019 r. GIIF przeprowadził 20 kontroli w następujących instytucjach obowiązanych:

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

- adwokaci – 2,
- banki – 2,
- biura usług płatniczych – 1,
- doradcy podatkowi – 2
- instytucje płatnicze – 1,
- notariusze – 3,
- podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług w zakresie wymiany pomiędzy walutami wirtualnymi – 1,
- pośrednicy w obrocie nieruchomościami – 5,
- radcowie prawni – 2,
- towarzystwa funduszy inwestycyjnych – 1.

Dodatkowo, w 2019 r. GIIF przeprowadził zdalne czynności kontrolne, tzw. *kontrole off-site* w: jednym banku, dwóch podmiotach prowadzących działalność w zakresie usługowego prowadzenia ksiąg rachunkowych oraz dwóch instytucjach płatniczych (łącznie 5 takich kontroli).

Z zakresie efektów działań w 2019 r., które stały się podstawą do skierowania przez Generalnego Inspektora zawiadomienia o przestępstwach opisanych z ustawie AML/CFT urząd podaje dane, iż skierował do prokuratury 1 zawiadomienie o popełnieniu przestępstwa wyczerpującego znamiona czynów określonych w art. 156 ustawy AML/CTF[53].

Natomiast w 2020 r. GIIF przeprowadził 7 kontroli w następujących instytucjach obowiązanych:

- banki – 3,
- notariusze – 2,
- podmiot rynku hazardowego – 1,
- towarzystwo funduszy inwestycyjnych – 1.

Ponadto w 2020 r. GIIF w związku z przeprowadzoną kontrolą, skierował do prokuratury **4 zawiadomienia** o podejrzeniu popełnienia przestępstwa wyczerpującego znamiona czynów określonych w art. 156 oraz art. 157 ustawy AML/CTF[54].

Trudno na podstawie powyższych danych wyciągać wnioski. Z pewnością podkreślić należy rolę instytucji obowiązanych w całym systemie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Dla jego spójności, wszystkie elementy i działania, muszą ze sobą współgrać. Warto podkreślić, iż stabilność finansowana systemu zależy od jego podatności na przestępstwa z art. 299 i 165a k.k. W interesie wszystkich instytucji rynku jest, by Polska była odbierana jako

[53] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2019 r., k. 57.

[54] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2020 r., k. 55.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

wiarygodny partner biznesowy, ze stabilnymi i ugruntowanymi narzędziami prawnymi sankcjonującymi negatywne zachowania.

13.6. PODSUMOWANIE

Aktualne rozwiązania prawne wydają się globalnie ujmować problematykę zjawiska prania pieniędzy oraz finansowania terroryzmu. Karne instrumenty w rękach organów ścigania, mają skutecznie, choćby poprzez prewencję generalną pokazywać, iż patologiczne zachowania będą sankcjonowane proporcjonalnymi karami. Rozbudowany system administracyjnych dolegliwości wobec niewywiązujących się ze swoich obowiązków instytucji obowiązanych z pewnością będzie stanowił pierwsze antidotum na zwiększenie wrażliwości uczestników systemu na zakres działań jakie muszą podjąć. Jednak, chyba przedwcześnie mówić, iż aktualne regulacje zarówno administracyjne, jak i karne w sposób skuteczny będą sankcjonowały delikty związane niewykonywaniem obowiązków przez instytucje obowiązane i ich reprezentantów. Kolejne Dyrektywy AML, przy współpracy z państwami członkowskimi wypracują nowe rozwiązania lub też wskażą krytyczne obszary w zakresie których może dojść do nadużyć, a wtedy pojawić się może potrzeba nowelizacji zakresu ścigania czynów jakich mogą dopuścić się przedstawiciele instytucji obowiązanych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

LITERATURA

Adamczyk P., *Możliwości zastosowania technologii blockchain w sektorze finansowym,* „Rynek-Społeczeństwo-Kultura" 2018, nr 1(27).

Alińska A., *Alternatywne Finanse*, CeDuWu, Warszawa 2019.

Alińska A., *Mechanizmy stabilności systemu finansowego*, C.H. Beck, Warszawa 2016.

Amiti M., Shang-Jin W., *Fear of Service Outsourcing. Is It Justified?*, „IMF Working Paper" 2004, s. 6–7.

Babiarz S. i in., *Ordynacja podatkowa. Komentarz*, Warszawa 2019, s. 684.

Bajor B., Zalcewicz A., Byrski J., *Ustawa o usługach płatniczych. Komentarz*, wyd. II, Wolters Kluwer, red. J. Byrski, Warszawa 2021.

Bartosiewicz A., Smaga M., *E-kontrola podatkowa i jednolity plik kontrolny*, Warszawa 2018, s. 1.

Bhagwati J., Panagariya A., Srinivsan T.N., *The Muddles over Outsourcing*, „Journal of Economic Perspectives", nr 18 (4).

Bieniak J., Bieniak M., Nita-Jagielski G., *Kodeks spółek handlowych. Komentarz*, wyd. 7, C.H. Beck, Warszawa 2020.

Blicharz G., Oręziak B., Wielec M., *Rynek finansowy – zapobieganie przyczynom przestępczości*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa 2019.

Brexit and AML/CFT, *Shell Companies and Money Laundering*, Wydawnictwo SWD, 2019.

Brzeziński B. i in., 2*.2.2. Blokada rachunku bankowego* (w:) *Nowe narzędzia kontrolne, dokumentacyjne i informatyczne w prawie podatkowym*, red. B. Brzeziński i in., Warszawa 2018.

Brzostowska M., Dziedźwiedzka M., K*omentarz praktyczny, obowiązki biur rachunkowych w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu*, Lex/el, 2021.

Brzostowska M., *Poradnik, Ocena ryzyka prania pieniędzy przez klientów biura rachunkowego*, Lex/el, 2021.

Buk K., *„Pranie brudnych pieniędzy" pochodzących z korzyści związanych z popełnieniem czynów zabronionych skierowanych przeciwko obowiązkom podatkowym*, „Doradca Podatkowy" 2006, nr 5, s. 54,

Buk K., *Obowiązki notariusza na podstawie przepisów ustawy z dnia 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Rejent" 2018, nr 12 (332).

Capiga M., *Bezpieczeństwo instytucji finansowych jako instytucji obowiązanych w systemie przeciwdziałania praniu pieniędzy*, „Studia Ekonomiczne" nr 171., Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice 2014.

Dobrzańska A., *Polityka makroostrożnościowa banku centralnego*, Difin, Warszawa 2016.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Duke L.S., *Departament sprawiedliwości Stanów Zjednoczonych, Spółki Shell, praktyki korporacyjne i jak je odkryć*, ReaserchGate, 2019.

Duży J., *3. Pranie pieniędzy* (w:) *Zorganizowana przestępczość podatkowa w Polsce. Zwalczanie przestępczego nadużycia mechanizmów podatków VAT i akcyzowego*, Warszawa 2013.

Dyl M., Królikowski M. (red), Górski A., Kruszyńska J., Krzykwa K., Lewandowska K., Marczuk M., Mierzejewski M., Sątowska-Strycharczyk P., Strycharczyk Ł., Świątek Ł., *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz. Krótkie komentarze Becka*, C.H. Beck, Warszawa 2021.

Federowicz M., *O normatywnym pojęciu stabilności finansowej na rynku finansowym Unii Europejskiej w nowej architekturze nadzorczej*, „Studia Europejskie" 2017, nr 4.

Fierla A. (red.), Dec P. (w:) *Wokół finansjeryzacji. Wybrane zagadnienia, Rozdział III Rozwój sektora FinTech a tradycyjna bankowość – ujęcie ilościowe*, Oficyna Wydawnicza SGH, Warszawa 2018.

Fijałkowska A., *Pranie pieniędzy oraz finansowanie terroryzmu jako współczesne zagrożenia bezpieczeństwa powszechnego i obrotu gospodarczego*, Wyższa Szkoła Bezpieczeństwa w Poznaniu, Poznań, s. 181–182.

Firkowski S., *Zmiany w postępowaniu egzekucyjnym w administracji*, C.H. Beck, Warszawa 2020.

Fojcik-Mastalska E., *Bank centralny. Miejsce Narodowego Banku Polskiego w sieci bezpieczeństwa finansowego,* (w:) *Prawo finansowe*, red. R. Mastalski, E. Fojcik-Mastalska, Warszawa 2011.

Folwarski M., *Sektor FinTech na europejskim rynku usług bankowych*, Poltex, Warszawa 2019.

Gareiss R., *Analysing the Outsourcers*, 2002-11-18 (data dostępu: 13.05.2010).

Gartner highlights outsourcing problems, 2005.

Gawron O., *Otoczenie regulacyjne sektora FinTech na przykładzie dyrektywy PSD2 i wybranych ustaw krajowych*, „Finanse i Prawo Finansowe" 2019, vol. 4(24).

Gay Ch.L.: *Outsourcing strategiczny: koncepcja, modele i wdrażanie*, Oficyna Ekonomiczna, Kraków 2002.

Ghamari M. El, *Finansowanie terroryzmu międzynarodowego* (w:) *Pieniądz i jego oddziaływanie na otoczenie*, red. P. Sitek, Warszawa 2016.

Ghamari M. El, *Przeciwdziałanie finansowania terroryzmu międzynarodowego* (w:) *Pieniądz i jego oddziaływanie na otoczenie*, red. P. Sitek, Warszawa 2016.

Głąba P.M., *Prawo jednostki do rozpoznania sprawy administracyjnej bez nieuzasadnionej zwłoki*, „Admin." 2011, nr 1.

Golonka A., *Polskie regulacje karne wobec „szóstej" dyrektywy Anti-Money Laundering*, „IUSNOVUM" 2021, nr 1.

Golonka A., *Przeciwdziałanie praniu pieniędzy w obliczu zmian wprowadzonych IV i V dyrektywą AML*, „Przegląd Ustawodawstwa Gospodarczego" 2020, nr 4.

Golonka A., *Zakres podmiotowy ustawy o przeciwdziałaniu praniu pieniędzy w świetle znowelizowanych przepisów*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2020, nr 82(3).

Gołębiewski P., *Bank jako instytucja zaufania publicznego (rozdział V), Prawne gwarancje bezpieczeństwa bankowego (rozdział VI), Nadzór nad stabilnością systemu bankowego*

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

(rozdział VII) (w:) *Prawo bezpieczeństwa finansowego. Wybrana problematyka*, red. M. Karpiuk, M. Sawicka, P. Sitek, Olsztyn 2016.
Gołębiewski P., *Ramy prawne blokady rachunku bankowego i wstrzymania transakcji płatniczej* (w:) *Pieniądz i jego oddziaływanie na otoczenie*, red. P. Sitek, recenzowana praca zbiorowa, Warszawa 2016.
Gołębiewski P., *System przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w Polsce* (w:) *Wyzwania i szanse dla polskiego sektora bankowego*, red. P. Sitek, recenzowana praca zbiorowa, Warszawa 2016.
Gołębiewski P., *Wpływ AML na sektor usług rachunkowych*, Kortowski Przegląd Prawniczy Uniwersytetu Warmińsko-Mazurskiego w Olsztynie, Olsztyn 2019.
Gołębiowska E., Jasiński W., Odziomek J., Wójcik J.W., *Zadania instytucji obowiązanych w przeciwdziałaniu praniu pieniędzy. Poradnik dla instytucji obowiązanych*, Warszawa 2001.
Górka J., Banki, *GAFAM, FinTech w gospodarce współdzielenia – equilibrium współpracy i konkurencji*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 531, Wrocław 2018.
Grabowska K., *MK Monitor księgowego wydanie specjalne. Przeciwdziałanie praniu brudnych pieniędzy oraz finansowaniu terroryzmu*, Inforlex, Warszawa 2019.
Grajcar K., *Limit płatności gotówkowych w świetle ustawy o przeciwdziałaniu praniu pieniędzy (AML)*, „Parkiet" 2021, nr 6.
Grudzewski W.M., Hejduk I.K., *Projektowanie systemów zarządzania*, Difin, Warszawa 2004.
Grycuk A., *Klastry a rozwój regionalny. Klaster usług biznesowych w Krakowie*, „Studia BAS" 2017, nr 1 (49), s. 144.
Grzywacz J., *Skuteczność instrumentów przeciwdziałających w Polsce procederowi prania brudnych pieniędzy*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej w Płocku. Nauki Ekonomiczne, nr 21, Płock 2015.
Hołda A., *Instrukcje księgowe i podatkowe. Rozdział I. Wewnętrzna procedura instytucji obowiązanej oraz zgłoszenie beneficjenta rzeczywistego do CRBR*, wyd. 2, C.H. Beck, Warszawa 2020.
Infor Pl, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu – nowe procedury*, Infor Pl, 2018.
Instrukcje księgowe i podatkowe, red. A. Hołda, wyd. 2, C.H. Beck, Warszawa 2020.
Ivana KiendlKrišto and Elodie Thirion Ex-Post Evaluation Unit and European Added Value Unit .
Jancisc D., *Shell Companies and Government Coruption*, Springer International Publishing AG, part of Springer Nature 2018.
Jurkowska-Zeidler A., *Bezpieczeństwo rynku finansowego w świetle prawa Unii Europejskiej*, Warszawa 2008.
Kapica W. (red.), B. Paxford, R. Obczyński, M. Gawroński, W. Kapica, M. Ćwiakowski, J. Grynfelder, W. Ługowski, A. Otto, E. Patsiotos, Z. Piotrowska, J. Stolarczyk, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik*, Wolters Kluwer, Warszawa 2018.
Kapica W., Grynfelder J., Ługowski W., Mierzwiński T., Obczyński R., Otto A., Patsiotos E., Piotrowska Z., Rycerski A., Stolarczyk J., *Przeciwdziałanie praniu brudnych*

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

pieniędzy i finansowaniu terroryzmu komentarze praktyczne, Wolters Kluwer, Warszawa 2020.
Kapica W., *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Wolters Kluwer, Warszawa 2020.
Karin J., *Spojrzenie za korporacje*, „SoFi" 2021, nr 7.
Karpiuk *M., Pranie pieniędzy jako zjawisko zagrażające bezpieczeństwu i porządkowi publicznemu* (w:) *Problematyka polskiego pieniądza*, red. P. Sitek, Warszawa 2015.
Kaseja K., *Podmioty uprawnione do dokonania blokady rachunku lub wstrzymania transakcji*, 2018, z. 3 (31).
Kasprzyk K., *Mechanizm podzielnej płatności*, Warszawa 2018.
Kenin H., *A look Behind Shell Corporation*, „Voices" 2021, nr 7.
Kenton W., Jomes M., *Shell Corporation*, 24 października 2020.
Kędzierski M., *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,* „Prokuratura i Prawo" 2021, nr 5.
Kędzierski M.A., „Prokuratura i Prawo" 2021, nr 5.
Kędzierski M.A., *Notariusz jako instytucja obowiązana w rozumieniu ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (omówienie niektórych zagadnień)*, „Studia Prawnicze KUL" 2020, nr 1, s. 165–195.
Kędzierski M.A., *Obowiązki i odpowiedzialność oficera AML (AMLO) w instytucji obowiązanej, cz. 1,* „Prokuratura i Prawo" 2021, nr 5, s. 66–91.
Kędzierski M.A., *Obowiązki i odpowiedzialność oficera AML (AMLO) w instytucji obowiązanej, cz. 2*, „Prokuratura i Prawo" 2021, nr 6, s. 45–72.
Kędzierski M.A., *Przeciwdziałanie i Zwalczanie Finansowania Terroryzmu w Polsce*, Wydawnictwo Adam Marszałek, Toruń 2019.
Kędzierski M.A., *Przeciwdziałanie i zwalczanie finansowania terroryzmu w Polsce*, Wydawnictwo Adam Marszałek, Toruń 2021.
Kędzierski M.A., *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22 (12).
Kocoń K., *Prawnopodatkowe aspekty pozyskiwania kapitału w ramach finasowania społecznościowego przez mikro i małe przedsiębiorstwa, Finanse, Rynki Finansowe*, „Ubezpieczenia" 2017, nr 4 (88), cz. 2, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego 2020.
Kodeks karny, Komentarz, wyd. 2, red. V. Konarska-Wrzosek, Wolters Kluwert, Warszawa 2020.
Kodeks karny, t. III: *Komentarz do art. 278–363 k.k., Komentarz do art. 299 k.k., pkt.7*, red. A. Zoll,
Kodeks karny. Komentarz aktualizowany, red. M. Mozgawa, LEX/el, 2021.
Kodeks karny. Komentarz, red. A. Grześkowiak, K. Wiak, wyd. 7, C.H. Beck, Warszawa 2021.
Kodeks spółek handlowych. Komentarz, red. Z. Jara, wyd. 3, C.H. Beck, Warszawa 2020.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Kozioł-Nadolna K., *Crowdfunding jako źródło finansowania innowacyjnych projektów,* Finanse, Rynki Finansowe, Ubezpieczenia, Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 73, Szczecin 2015.

Krasuski A., *Korzystanie z chmury obliczeniowej przez instytucje w świetle RODO*

Kraszewski A., Krzal K. (w:) *Prawo przedsiębiorców. Komentarz*, *art. 62*, red. A. Pietrzak, Warszawa 2019.

Krysiński Ł., *Odkrywanie tajemnic kont bankowych*, „Prokuratura i Prawo" 2021, nr 4.

Kuijlen T., Migut G., *Wykrywanie nadużyć i pranie brudnych pieniędzy*, StatSoft 2004.

Lemmonier M., *Europejskie modele instrumentów finansowych*, Wolters Kluwer, Warszawa 2017.

Leżoń K., *Otwarta bankowość w świetle wymogów Dyrektywy PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech*, Publikacja Komisji Nadzoru Finansowego, Warszawa 2019.

Lizak R., *Pranie pieniędzy w prawie polskim na tle europejskim, międzynarodowym i amerykańskim*, C.H. Beck, Warszawa 2018.

Łoboda M., Strzelec D., *1.3. Zadania Krajowej Administracji Skarbowej* (w:) *Kontrola przestrzegania przepisów prawa podatkowego*, M. Łoboda, D. Strzelec, Warszawa 2017.

Łoboda M., Strzelec D., *1.3.4. Zadania w zakresie zwalczania przestępczości* (w:) M. Łoboda, W. Ługowski, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz, art. 72*, red. W. Kapica, Warszawa 2020.

Majewski K., *Zmiany w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,* „Monitor Prawa Bankowego" 2020, nr 1, s. 92–103.

Małolepszy M., Pierzchlewicz M., *Odpowiedzialność karna oficera compliance*, „Prokuratura i Prawo" 2019, nr 5.

Marek A., *Kodeks karny. Komentarz. Komentarz do art. 299 kodeksu karnego,* pkt 2, LEX, 2010.

Martysz C., Walczak K., *Zarys problematyki przeciwdziałania przestępstwom gospodarczym i ich wykrywania*. Szkoła Główna Handlowa w Warszawie, Warszawa 2018.

Matejun M., *Outsourcing* (w:) *Kompendium metod i technik zarządzania. Teoria i ćwiczenia*, red. K. Szymańska, Oficyna a Wolters Kluwer business, Warszawa 2015.

Matusiakiewicz Ł., *Obowiązkowy split payment*, Warszawa 2019, s. 23.

Milic-Czerniak R., *Rola FinTechów w rozwoju innowacji finansowych, Studia BAS*, nr 1(57), Biuro Analiz Sejmowych, Warszawa 2019.

Morek R. (w:) *Kodeks cywilny.., t. 3b*, kom. do art. 734, nr 1, red. K. Osajda, 2017.

Nalepka A., *Restrukturyzacja przedsiębiorstw*, PWN, Warszawa–Kraków 1999.

Niezgódka-Medek M. (w:) *Ordynacja podatkowa. Komentarz, art. 119(zha)*, wyd. XI, S. Babiarz, B. Dauter, R. Hauser, A. Kabat, J. Rudowski, M. Niezgódka-Medek, Warszawa 2019.

Notaries of Europe Providing legal certainty*, Zwalczanie prania pieniędzy. Walka globalna,* Wyzwanie Dla Europy, 2020, nr 2.

Nowakowski M., *FinTech, technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji*, Wolter Kluwer, Warszawa 2020.

Obuchowicz M., *Pięć lat funkcjonowania Centrum Antyterrorystycznego ABW (2008–2013)*, PBW nr 10, 2014, s. 275.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Ochnio A.H., *Blokada rachunku i wstrzymanie transakcji jako środki przymusu w procesie karnym*, Wolters Kluwer, Warszawa 2015.

Opitek P., *Pranie, Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12.

Ożóg I., *Karuzele i inne oszustwa podatkowe. Metody przeciwdziałania unikaniu opodatkowania*, Wolters Kluwer, Warszawa 2021.

Pabiański T., Śliż W., *Zorganizowane działanie przestępcze wykorzystujące mechanizmy konstrukcyjne podatku VAT, cz. 1*, Wolters Kluwer, „Przegląd Podatkowy" 2007, nr 1, s. 18–27.

Patsiotos E. (w:) *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Warszawa 2020,

Penc J., *Leksykon biznesu*, Placet, Warszawa 1997.

Pieniądz i jego oddziaływanie na otoczenie, red. P. Sitek, Warszawa 2016.

Pływaczewski E., *Proceder prania pieniędzy i jego implikacje*, LEX, 2013.

Podsiadły A., Zawiejska-Rataj J., *Rozpoznawanie, wykrywanie, ściganie i zwalczanie czynów zabronionych, zapobieganie im i ściganie ich sprawców przez organy Krajowej Administracji Skarbowej*, „Przegląd Podatkowy" 2017, nr 10, s. 37–42.

Pokrzywdzony jako uczestnik postępowań represyjnych. Czwarty wierzchołek trójkąta?, red. P. Czarnecki, C.H. Beck, Warszawa 2021.

Prawo bezpieczeństwa finansowego, red. P. Sitek, M. Karpiuk, M. Sawicka, Warszawa 2016.

Prawo Karne Gospodarcze, System Prawa Handlowego, t. 10, wyd. 2, red. R. Zawłocki, C.H. Beck, Warszawa 2018.

Prawo karne, red. A. Grześkowiak, K. Wiak, C.H. Beck, Warszawa 2020.

Prawo rynku finansowego. Doktryna, instytucje, praktyka, red. A. Jurkowska-Zeidler, M. Olszak, Warszawa 2016.

Prengel M., *Środki zwalczania przestępczości prania pieniędzy w ujęciu prawno-porównawczym*, TNOiK, Toruń 2003.

Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu, Komentarz, red. W. Kapica, Wolters Kluwer, Warszawa 2020.

Rajewska J., Strzelecka M*., Praktyczne aspekty stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień*, 2020.

Rogowski W. *Błędna „5" outsourcingu*. „CIO Magazyn Dyrektorów IT" 2006.

Sawicki M., *Wpływ pandemii (Covid-19) na zamianę modeli biznesowych na przykładzie branży bankowej w Polsce*, Zeszyty Naukowe ZPSB Firma i Rynek, nr 1 (59), Szczecin 2021.

Siejczuk P., *Problematyka prania brudnych pieniędzy w regulacjach prawnomiędzynarodowych, europejskich i krajowych*, „Bezpieczeństwo Narodowe" 2012, nr III–IV.

Sikorski G., *Prawo bankowe, komentarz*, C.H. Beck, Warszawa 2015.

Sitek P., *Polityka pieniężna Narodowego Banku Polskiego i Europejskiego Banku Centralnego w obliczu kryzysu finansowego i po kryzysie* (w:) *Wpływ prawa Unii Europejskiej na gospodarkę i samorząd terytorialny państw członkowskich*, red. M. Ganczar, J. Król, M. Szewczak, Wydawnictwo Afinance, Łódź 2017.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Sitek P., *Przeobrażenia systemu bankowego w kontekście utworzenia unii bankowej*, Wyższa Szkoła Finansów i Zarządzania, Warszawa 2017
Sitek P., *The economic security of the State and the banking union*, Lambert Academic Publishing, 2015.
Sitek P., *Wpływ skali i struktury finansowania, sektora przedsiębiorstw, na gospodarkę…* (w:) *Sytuacja prawno-finansowa przedsiębiorców sektora małych i średnich przedsiębiorstw*, red. A. Niemczyk-Wójcik, T. Talar, Warszawa 2016.
Sitek P., *Zintegrowany sektor bankowy Unii Europejskiej. Studium prawno-finanso*we, Vizja Press & IT, Warszawa 2015.
Smolak M., *Formy zwalczania procederu prania brudnych pieniędzy*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 13 s. 294.
Sroga A., *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Obowiązki biur rachunkowych*, Infor, 2021.
Staniszewski M., *Egzekucja administracyjna obowiązków o charakterze niepieniężnym*, Studia Administracyjne, nr 10, Szczecin 2018.
Strzelec D., *Kontrola przestrzegania przepisów prawa podatkowego*, Wolters Kluwer, Warszawa 2017.
System prawa karnego, t. 9: *Przestępstwa przeciwko mieniu i gospodarcze*, red. R. Zawłocki, Warszawa 2015, s. 586.
Systemy zarządzania zgodnością. Compliance w praktyce, red. B. Jagura, B. Makowicz, WKP, 2020.
Szczepańska O., *Stabilność finansowa jako cel banku centralnego*, Wydawnictwo Naukowe Scholar, Warszawa 2008.
Szereda A.J., *Notariat. Czynności Notarialne. Wydanie I. Środki bezpieczeństwa finansowego,* C.H. Beck, Warszawa 2021.
Szurek M., *Pozyskiwanie śladów finansowania terroryzmu i ich przetwarzanie*, Gdańskie Wydawnictwo Oświatowe, Gdańsk 2021.
Szydło S., *Problemy stabilizacji polskiej gospodarki w okresie rynkowych reform*, Wydawnictwa Naukowe AGH, Kraków 2013.
Szydło S., *Rola państwa w kształtowaniu stabilnego, efektywnego systemu finansowego*, Studia Ekonomiczne / Uniwersytet Ekonomiczny w Katowicach, nr 210, Katowice 2015.
Teszner K., *Ordynacja podatkowa. Komentarz aktualizowany, art. 119(zv)*, Warszawa 2021.
Torończak M., *Komitet Stabilności Finansowej po zmianach*, „Monitor Prawa Bankowego" 2017, nr 5.
Trocki M., *Outsourcing*, PWE, Warszawa 2001.
Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz, red. M. Dyl, M. Królikowski, C.H. Beck, Warszawa 2021.
Walczak P., *Dokumentacja wewnętrzna w jednostkach sektora finansów publicznych*, C.H. Beck, Warszawa 2020.
Wodecka-Hyjek A., Zeszyty Naukowe nr 775, Uniwersytet Ekonomiczny w Krakowie, Kraków 2008.
Wolfsberg statement on AML Screening/Monitoring and Serching 2009, GrupaWolfsberg, 2009.
Wójcik J.W., *Pranie pieniędzy. Kryminologiczna ocena transakcji w procesie prania pieniędzy*, Twigger, Warszawa 2002 s. 133.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Wójcik J.W., *Przeciwdziałanie finansowaniu terroryzmu*, Wolters Kluwer, Warszawa 2007, s. 70.
Żygadło A., *Usługa cloud computingu jako czynność faktyczna związana z działalnością bankową*, „Monitor Prawa Bankowego" 2013, nr 7–8, s. 83–94.

WYKAZ ŹRÓDEŁ PRAWA

Akty prawa międzynarodowego

Karta Narodów Zjednoczonych, podpisana dnia 26 czerwca 1945 r. w San Francisco (data obowiązywania 24 października 1945 r.).
Konwencji Rady Europy z dnia 16 maja 2005 r. – o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu (Dz.U. z 2008 r., nr 165, poz. 1028).

PRAWO UNII EUROPEJSKIEJ

Traktaty UE

Traktat o funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r. (Dz.U.z 2004 r., 90.864/2) (wersja skonsolidowana Dz. Urz. UE C 400 z dnia 7 czerwca 2016 r., s. 11).
Traktat o Unii Europejskiej z dnia 7 lutego 1992 (Dz.U. z 2004 r., 90.864/30) (wersja skonsolidowana Dz. Urz. UE C 202 z dnia 7 czerwca 2016 r., s. 13).

Dyrektywy Unii Europejskiej

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. UE. L. z 2015 r., nr 337, s. 35 z późn. zm.).
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.
Dyrektywa Parlamentu Europejskiego I Rady (UE) 2018/1673 z dnia 23 października 2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Rozporządzenie UE

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Inne:

COM(2021) 422 fina. Proposal for a Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-assets (Recast). Brussels, 20 lipca 2021.

Resolution CM/Res(2013)13 on the Statute of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) (Adopted by the Committee of Ministers on 9 October 2013 at the 1180th meeting of the Ministers' Deputies).

Rezolucja Parlamentu Europejskiego z dnia 17 maja 2017 r. w sprawie FinTech: wpływ technologii na przyszłość sektora finansowego (2016/2243(INI)) (Dz.U. UE. C. z 2018 r., nr 307).

Wniosek Rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniającedyrektywę (UE) 2019/193, Bruksela, dnia 24 września 2020 r., COM(2020) 593 final, 2020/0265(COD).

PRAWO RZECZYPOSPOLITEJ POLSKIEJ

Źródła prawa polskiego

Ustawa z dnia 23 kwietnia 1964 r., Kodeks cywilny (t.j. Dz.U. z 2020 r., nr 0, poz. 1740).

Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (t.j. Dz.U. z 2020 r., poz. 1427 ze zm.).

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2020 r., poz. 1320).

Ustawa z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz.U. z 2020 r., 1651).

Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (Dz.U. z 2020 r., 75).

Ustawa z dnia z dnia 14 lutego 1991 r. Prawo o notariacie (Dz.U. z 2020 r., 1192).

Ustawa z dnia 12 października 1994 r. o ochronie obrotu gospodarczego i zmianie niektórych przepisów prawa karnego (Dz.U. nr 126, poz. 615).

Ustawa z dnia 5 lipca 1996 r. o doradztwie podatkowym (Dz.U. z 2020 r., 130).

Ustawa z dnia 2 kwietnia 1997 r., Konstytucja Rzeczypospolitej Polskiej (Dz.U. z 1997 r., nr 78, poz. 483).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2020 r., poz. 1444).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. z 1997 r., nr 89, poz. 555).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Ustawa z dnia 21 sierpnia 1997 r. o Gospodarce Nieruchomościami (Dz.U. z 2020 r., poz. 11, 234 i 815).
Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (t.j. Dz.U. z 2020 r., poz. 2027).
Ustawa z dnia 29 sierpnia 1997 r., Ordynacja podatkowa (Dz.U. z 1997 r., nr 137, poz. 926).
Ustawa z dnia 29 sierpnia 1997 r., Prawo bankowe (Dz.U. 1997 nr 140 poz. 939).
Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (tj. Dz.U. z 2020 r., poz. 1526, 2320).
Ustawa z dnia 27 lipca 2002 r. Prawo dewizowe (Dz.U. z 2002 r., nr 141, poz. 1178).
Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz.U. z 2020 r., poz. 358).
Ustawa z dnia 29 lipca 2005 r., o nadzorze nad rynkiem kapitałowym (Dz.U. z 2005 r., nr 183, poz. 1537).
Ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (Dz.U. z 2020 r., poz. 2080 oraz z 2021 r., poz. 355).
Ustawa z dnia 5 listopada 2009 r., o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. z 2012 r., poz. 855).
Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r., 1130).
Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2021 r., poz. 1132).
Ustawa z dnia 6 marca 2018 r. Prawo Przedsiębiorców (Dz.U. z 2021 r., poz. 162).
Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r., poz. 815).

Rozporządzenia

Rozporządzenie Ministra Finansów z dnia 16 maja 2018 r. w sprawie odbierania zgłoszeń naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., 959).
Rozporządzenie Ministra Finansów z dnia 16 maja 2018 r. w sprawie wniosków o udostępnienie informacji o beneficjentach rzeczywistych oraz udostępniania tych informacji (Dz.U. z 2018 r., poz. 965).
Rozporządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 13 listopada 2020 r. w sprawie szczegółowego zakresu informacji oraz rodzaju i formy dokumentów dołączanych do wniosku o wydanie zezwolenia na prowadzenie działalności w charakterze krajowej instytucji płatniczej (Dz.U. z 2020 r., poz. 2225).

Inne źródła

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Kształtowanie cyfrowej przyszłości Europy", COM(2020) 67 final, 19 lutego 2020 r.
Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Plan działania w zakresie technologii finansowej", COM(2018) 109 final, 8 marca 2020 r.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Decydujący moment dla Europy: naprawa i przygotowanie na następną generację", COM(2020) 456 final, 24 września 2020 r.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „W sprawie strategii dla UE w zakresie finansów cyfrowych", COM(2020) 591 final, 24 września 2020 r.

Komunikat nr 22 Ministerstwa Finansów z dnia 07 kwietnia 2020 r. w sprawie praktycznych aspektów stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień, o których mowa w art. 74 i art. 86 ustawy AML.

Krajowa Ocena Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu, Ministerstwo Finansów, Warszawa, 2019 r.

Money Laundering Control Act of 1986 (USA).

Pismo z dnia 12 stycznia 2020 r. Urząd Komisji Nadzoru Finansowego, Ostrzeżenie o ryzykach związanych z nabywaniem oraz z obrotem kryptoaktywami (w tym walutami wirtualnymi oraz kryptowalutami).

Pismo z dnia 27 stycznia 2015 r. Generalny Inspektor Informacji Finansowej Komunikat GIIF dotyczący zasad rejestracji transakcji.

Projekt Rezolucji w sprawie kompleksowej unijnej polityki zapobiegania praniu pieniędzy i finansowaniu terroryzmu – plan działania Komisji i dalszy rozwój sytuacji, 1 lipca 2020 r., https://www.europarl.europa.eu/doceo/document/B-9-2020-0207_PL.html (data dostępu: 25 sierpnia 2021).

Publikacja Komisji Nadzoru Finansowego „Cyfrowa Agenda Nadzoru" – plan działań Urzędu KNF w zakresie m.in. nowoczesnych technologii, innowacji oraz cyberbezpieczeństwa, Warszawa, dnia 19 grudnia 2019 r.

Publikacja Narodowego Banku Centralnego, Departament Systemu Płatniczego NBP Warszawa, maj 2021 r., Pieniądz cyfrowy banku Centralnego.

Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2019 r.

Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2020 r.

Sprawozdanie Głównego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2020 r., Warszawa, marzec 2021 r.

Stanowisko UKNF dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnieniem w działalności banków, Warszawa, 16 września 2019.

Uchwała nr 50 Rady Ministrów z dnia 19 kwietnia 2021 r. w sprawie przyjęcia strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (M.P. z 2021 r., poz. 435).

Uzasadnienie Prezesa Rady Ministrów z 26 października 1999 r. do Ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł, druk sejmowy III kadencji, nr 1478.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Wytyczne w sprawie outsourcingu z dnia 25 lutego 2019 r. Europejski Urząd Nadzoru Bankowego EBA/GL/2019/02.

Zarządzenie nr 5/2021 Przewodniczącego Komisji Nadzoru Finansowego z dnia 22 lutego 2021 r., w sprawie nadania regulaminu organizacyjnego Urzędowi Komisji Nadzoru Finansowego.

Źródła internetowe

"What are the Legal Risks to Cryptocurrency Investors? Nathan Reiff, June 25 2019, https://www.investopedia.com/tech/what-are-legal-risks-cryptocurrency-investors/ (data dostępu: 10 września 2021).

ABW, https://www.abw.gov.pl/pl/informacje/1848,ABW-rozbila-quotpralniequot-pieniedzy.html (data dostępu: 19 września 2021).

Ajs M., Widzewicz A., Rozszerzenie odpowiedzialności za naruszenie obowiązków dotyczących przeciwdziałania praniu pieniędzy, https://www.prawo.pl/ biznes/wieksza–odpowiedzialnosc–i–wyzsze–kary–za–naruszenie–obowiazkow, 496338.html, 2019.

Artificial Intelligence Will Enable 38% Profit Gains By 2035, https://www.forbes.com/sites/louiscolumbus/2017/06/22/artificial-intelligence-will-enable-38-profit-gains-by-2035/?sh=5665610e1969#:~:text=bran%C5%BCy%20.%20Raport%20mo%C5%BCna-,pobra%C4%87%20tutaj,-(28%20s.%2C%20PDF (data dostępu: 19 sierpnia 2021).

Bartosiewicz M., AML: znaczące zmiany zbliżają się wielkimi krokami, www.rp.pl/prawo-w-firmie/art8656781-aml-znaczace-zmiany-zblizaja-sie-wielkimi-krokami (data dostępu: 10 września 2021).

Co to jest Internet Rzeczy (IoT)?, https://www.benchmark.pl/aktualnosci/co-to-jest-internet-rzeczy-iot.html (data dostępu: 26 sierpnia 2021).

Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and The Committee of the Regions FinTech Action plan: For a More Competitive and Innovative European Financial Sector EN, https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf.

Digital Banking Maturity 2020, *Jaka jest reakcja banków na cyfrową rewolucję?*, https://www2.deloitte.com/pl/pl/pages/financial-services/articles/digital-banking-maturity-2020.html (data dostępu: 29 sierpnia 2021).

Egmont Group, https://www.egmontgroup.org/en/content/about (data dostępu: 22 sierpnia 2021).

European Innovation Scoreboard 2021 r., Publications Office of the European Union, Luxembourg 2021 r., https://ec.europa.eu/docsroom/documents/46013.

Fintek, Płatności odroczone, rozwój e-commerce i usługi chmurowe. Rok pandemii w sektorze FinTech, https://fintek.pl/platnosci-odroczone-rozwoj-e-commerce-i-uslugi-chmurowe-rok-pandemii-w-sektorze-fintech/ (data dostępu: 21 sierpnia 2021).

Gibas W., Zawiadomienie do Generalnego Inspektora Informacji Finansowej, https://pl.linkedin.com/pulse/zawiadomienie-do-generalnego-inspektora-informacji-finansowej-gibas (data dostępu: 24 sierpnia 2021).

GIIF: komunikat nr 11 w sprawie raportowania https://www.gov.pl/web/finanse/komunikat-nr-11-w-sprawie-raportowania-do-giif-informacji-o-transakcjach-ponadprogowych-o-ktorych-mowa-w-art-72-ust-1-pkt-1-i-2-ustawy-aml (data dostępu: 11 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

gov.pl, Wizyta ekspertów Komitetu MONEYVAL Rady Europy 10.05.2021, https://www.gov.pl/web/finanse/wizyta-ekspertow-komitetu-moneyval-rady-europy (data dostępu: 22 sierpnia 2021).

https://assets.kpmg/content/dam/kpmg/pl/pdf/2021/05/pl-pl-alert-kpmg-2020-05-17-nowelizacja-ustawy-o-przeciwdzialaniu-praniu-pieniedzy-oraz-finansowaniu-terroryzmu.pdf.

https://eur-lex.europa.eu/legal-content/PL/LSU/?uri=celex:32015L0849.

https://rpms.pl/dokumenty-aml/.

https://sanctionscanner.com/knowledge-base/money-laundering-reporting-officer-mlro-125.

https://www.iaml.com.pl/wiedza/obowiazki-instytucji-obowiazanych/.

https://www.knf.gov.pl/knf/pl/komponenty/img/Prezentacja%20CEDUR%2016-05-2018_61908.pdf (data dostępu: 25 sierpnia 2021).

Internetowy System Aktów Prawnych (ISAP), https://isap.sejm.gov.pl/.

Jednolity Plik Kontrolny, https://www.podatki.gov.pl/jednolity-plik-kontrolny/jpk-vat-z-deklaracja/jpk-vat-z-deklaracja-info/ (data dostępu: 21 września 2021).

Kaczmarek P., Kary w AML – co nam grozi?, https://home.kpmg/pl/pl/blogs/home/posts/2021/05/blog-podatkowy-nowelizacja-ustawy-o-aml-uchwalona-30-marca-2021-roku-i-jej-wplyw-na-instytucje-obowiazane.html.

Kędzierski M.A., *Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, http://www.abw.gov.pl/download/1/2984/MKedzierski-POL.pdf.

Komisja Europejska, *Digital finance package*, https://ec.europa.eu/info/publications/200924-digital-finance-proposals_pl.

Komisja Nadzoru Finansowego, *Rekomendacje H dotycząca systemu kontroli wewnętrznej w bankach*, https://www.knf.gov.pl/knf/pl/komponenty/img/knf_170534_Rekomendacja_H_2017_50303.pdf, 2017.

Komunikat nr 22 w sprawie praktycznych aspektów stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień, o których mowa w art. 74 i art. 86 ustawy AML, https://www.gov.pl/web/finanse/komunikat-nr-22-w-sprawie-praktycznych-aspektow-stosowania-srodkow-bezpieczenstwa-finansowego-oraz-przekazywania-zawiadomien-o-ktorych-mowa-w-art-74-i-art-86-ustawy-aml2.

Komunikat nr 8 w sprawie nadawania nazw plikom przekazywanym przez instytucje obowiązane do GIIF, zawierającym informacje o transakcjach ponadprogowych, o których mowa w art. 72 ustawy AML.

Luka w VAT, https://demagog.org.pl/wypowiedzi/luka-vat-w-polsce-sprawdzamy-dane-nik/ (data dostępu: 21 września 2021).

Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz Proliferacji Rekomendacje FATF, Urząd Komisji Nadzoru Finansowego, tłum. R. Obczyński (Departament Inspekcji Bankowych i Instytucji Płatniczych, Wydział Przeciwdziałania Praniu Pieniędzy), https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacje_FATF_40223.pdf (data dostępu: 19 sierpnia 2021).

Milczanowski S., Sałdan K., Co się zmieni w obowiązku identyfikacji beneficjentów rzeczywistych?, https://www.dzp.pl/blog/compliance/co-sie-zmieni-w-obowiazku-identyfikacji-beneficjentow-rzeczywistych/ (data dostępu: 8 września 2021).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Ministerstwo Finansów, Zgłoszenie informacji o beneficjentach https://www.gov.pl/web/finanse/zgloszenie-informacji-o-beneficjentach.

Musiał K.J., Środki bezpieczeństwa finansowego, https://sip.lex.pl/procedury/srodki-bezpieczenstwa-finansowego-1610618975 (data dostępu: 7 lipca 2021).

Musiał K.J., Zgłaszanie informacji o beneficjentach rzeczywistych, https://sip.lex.pl/procedury/zglaszanie-informacji-o-beneficjentach-rzeczywistych-1610618941 (data dostępu: 7 września 2021).

NIK, *Informacja o wynikach kontroli*, https://www.nik.gov.pl/plik/id,3369,vp,4270.pdf (data dostępu: 19 września 2021).

Nowelizacja ustawy AML dotycząca implementacji Dyrektywy V AML, Jakie zmiany przyniosła nowelizacja ustawy AML z 2021 roku, związana z implementacją Dyrektywy V AML?, https://www.iaml.com.pl/wiedza/nowelizacja-ustawy-aml-implementacja-dyrektywy-v-aml/ (data dostępu: 8 września 2021).

Piech A.K., Ministerstwo Cyfryzacji, Warszawa 2016, kryptochemik.pl.

PortfelInternetowy.com, Neo Banki – dowiedz się czym są fintech i jakie niosą korzyści, https://www.portfelinternetowy.com/neo-banki-dowiedz-sie-czy-sa-fintech-i-jakie-niosa-korzysci (data dostępu: 21 sierpnia 2021).

Przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmowi, https://www.gov.pl/web/finanse/przeciwdzialanie-praniu-pieniedzy-i-finansowaniu-terroryzmu (data dostępu: 3 września 2021).

Raport of Tech.eu, *The State-of-European-Fintech*, January 2021, https://tech.eu/wp-content/uploads/woocommerce_uploads/2021/01/State-of-European-Fintech-0h4ee7.pdf (data dostępu: 21 sierpnia 2021).

Raport Płatności cyfrowe 2020, https://eizba.pl/wp-content/uploads/2020/12/Raport-Platnosci-cyfrowe-2020-10.12.2020.pdf, s. 11.

Recommendation 18: Internal controls and foreign branches and subsidiaries, https://cfatf-gafic.org/index.php/documents/fatf-40r/384-fatf-recommendation-18-internal- controls-and-foreign-branches-and-subsidiaries (data dostępu: 19 sierpnia 2021).

Serwis Rzeczypospolitej Polskiej, *Generalny Inspektor Informacji Finansowej*, https://www.gov.pl/web/finanse/centralny-rejestr-beneficjentow-rzeczywistych (data dostępu: 19 sierpnia 2021).

Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/mswia/giif (data dostępu: 10 września 2021).

Siejczuk P., *Problematyka prania brudnych pieniędzy w regulacjach prawnomiędzynarodowych, europejskich i krajowych*, http://www.bbn.gov.pl/ (data dostępu: 21 sierpnia 2021).

Social.Estate, *FinTech*, https://social.estate/slownik/FinTech-co-to-jest/ (data dostępu: 20 lipca 2021).

Sprawozdanie GIFF za 2020 r., file:///C:/Users/admin/Downloads/Sprawozdanie_GIIF_za_2020_r_.pdf (data dostępu: 19 września 2021).

Sprawozdanie zawierające zalecenia dla Komisji w sprawie finansów cyfrowych: pojawiające się ryzyko związane z kryptoaktywami – wyzwania w zakresie regulacji i nadzoru w obszarze usług, instytucji i rynków finansowych (2020/2034(INL).

System analityczny AML, https://www.iaml.com.pl/system-analityczny/.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

System płatniczy, https://www.nbp.pl/home.aspx?f=/systemplatniczy/karty_platnicze.html, s. 1 (data dostępu: 16 sierpnia 2021).

Sztuczna inteligencja nie funkcjonuje bez danych, https://uodo.gov.pl/pl/138/2010.

Top10mobilebanks.com, *Top Mobile Banks in Europe*, https://top10mobilebanks.com/best-mobile-banks-dtop-t2/?edgetrackerid=100381575405706&gclid=CjwKCAjwyIKJBhBPEiwAu7zll2rVijTG3FsUWvUgRmWYdwRgyt8n1b1vYzIjMSOfuQWzjYfBfRPV3hoC_AQQAvD_BwE (data dostępu: 21 sierpnia 2021).

Uzasadnienie projektu ustawy o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw, https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=909 (data dostępu: 7 września 2021).

Zawadzki J., W poszukiwaniu beneficjenta rzeczywistego, https://www.parp.gov.pl/component/content/article/62251:w-poszukiwaniu-beneficjenta-rzeczywistego (data dostępu: 7 września 2021).

Zmiana przepisów o przeciwdziałaniu praniu pieniędzy. Nowe instytucje obowiązane i surowsze wymogi weryfikacji beneficjenta rzeczywistego, https://www.parp.gov.pl/component/content/article/73691:zmiana-przepisow-o-przeciwdzialaniu-praniu-pieniedzy-nowe-instytucje-obowiazane-i-surowsze-wymogi-weryfikacji-beneficjenta-rzeczywistego (data dostępu: 25 sierpnia 2021).

Orzecznictwo

Postanowienie Sądu Apelacyjnego w Krakowie – II Wydział Karny z dnia 9 listopada 2017 r. II AKz 414/17.

Wyrok Naczelnego Sądu Administracyjnego z dnia 3 grudnia 2020 r. II FSK 2185/18.

Wyrok Naczelnego Sądu Administracyjnego z dnia 4 marca 2014 r., sygn. II GSK 1996/12, Obowiązek rejestracji transakcji umów darowizny nieruchomości. Wykorzystanie transakcji darowizny nieruchomości w procesie prania pieniędzy.

Wyrok Sądu Apelacyjnego w Gdańsku z dnia 27 grudnia 2016 r., sygn. II AKa 163/16, Strona podmiotowa prania pieniędzy.

Wyrok Sądu Apelacyjnego w Katowicach z dnia 11 maja 2017 r., sygn. II AKa 42/17, Śmierć oskarżonego po wydaniu wyroku. Świadomość przestępczego pochodzenia pieniędzy jako warunek odpowiedzialności za pranie pieniędzy.

Wyrok Sądu Apelacyjnego w Poznaniu z dnia 11 marca 2015 r., sygn. II AKa 150/14, Przedmiot prania pieniędzy. Zakres zakazu prowadzenia działalności gospodarczej.

Wyrok Sądu Apelacyjnego w Warszawie z dnia 2 czerwca 2017 II AKa 156/17, Analiza znamion prania pieniędzy. – LEX nr 2317774

Wyrok Sądu Najwyższego z dnia 20 maja 2013 r., sygn. akt III K 455/12.

Wyrok SN z dnia 20 lipca 2006 r., V CSK 115/06, LEX nr 1044085.

Wyrok SN z dnia 23 stycznia 2008 r., V CSK 377/07.

Wyrok Trybunału Sprawiedliwości z dnia 17 stycznia 2018 r., sygn. C-676/16C-676/16, Działalność gospodarcza polegająca na sprzedaży spółek utworzonych wyłącznie w celu ich zbycia a przeciwdziałanie korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu., Corporate Companies s.r.o. v. Ministerstvo Financí ČR.

Wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 6 maja 2016 r. sygn. I SA/Kr 359/16.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 24 marca 2021 r., VI SA/Wa 2690/20, brak podstaw do odstąpienia od wszczęcia postępowania, LEX, nr 3209323.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 8 kwietnia 2014 r., sygn. VI SA/Wa 2645/13, Stosowanie środków bezpieczeństwa finansowego. Działanie przedsiębiorstw faktoringowych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376

Opracowanie przygotowane jest na dobrym poziomie naukowym, Autorzy właściwie charakteryzują instytucje służące przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Badania przeprowadzone w pracy oparte są na solidnym materiale źródłowym i stanowią ważny głos w dyskusji nad tytułowymi zagadnieniami, odnoszącymi się do zjawisk bezpośrednio zagrażających bezpieczeństwu państwa i jego obywateli.

prof. dr hab. Mirosław Karpiuk
Uniwersytet Warmińsko-Mazurski w Olsztynie

Wybór tematu określonego tytułem recenzowanej pracy zbiorowej jako przedmiotu eksploracji naukowej uważam za trafny, oryginalny i godny dociekań badawczych. Przedstawiono w niej zagadnienia dotyczące różnych aspektów systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, jak m.in. kontekst stabilności finansowej państwa, status oficera ds. zgodności z ustawą o przeciwdziałaniu praniu pieniędzy, problematykę identyfikacji beneficjenta rzeczywistego, outsourcing procesów związanych z AML/CFT czy rozwoju zautomatyzowanych technologii wspierających AML i CFT. Warto podkreślić, że praca, mimo iż składa się z trzynastu rozdziałów, jest spójna, co nie było z pewnością zadaniem łatwym, biorąc pod uwagę liczbę autorów i przedmiot badań. Dlatego należy docenić wyjątkowo staranną pracę redaktorów, którzy zadbali, aby każdy rozdział zawierał uwagi wprowadzające i podsumowanie, w ramach których konsekwentnie określano cel i przedmiot badań oraz formułowano wnioski. Szczególnym walorem recenzowanej pozycji jest także, a może przede wszystkim, to, iż każdy z Autorów dokonując egzegezy obowiązujących aktów normatywnych starał się wzbogacać jej rezultaty o własną i niejednokrotnie pogłębioną refleksję naukową, stawiając wiele niezwykle interesujących wniosków de lege ferenda. Monografia nie tworzy sztucznego konglomeratu luźno ze sobą związanych tekstów, lecz stanowi kompletny i systemowy efekt pracy badawczej, której wyniki mają wymiar nie tylko teoretyczny, lecz przede wszystkim praktyczny, albowiem mogą mieć one rzeczywisty wpływ, dzięki publikacji tej monografii, na zwiększenie w przyszłości odporności systemu finansowego na próby wykorzystania go w celach przestępczych.

dr hab. Jarosław Kostrubiec, prof. UMCS
Uniwersytet Marii Curie-Skłodowskiej w Lublinie

WYDAWNICTWO AEH

ISBN 978-83-66552-42-5

www.wydawnictwo.aeh.edu.pl

Plik zabezpieczony watermarkiem jawnym i niejawnym: 18361193A3237376